HIRSCHMANN

User Manual

Industrial ETHERNET Firewall
EAGLE mGuard

Technical Support
HAC-Support@hirschmann.de

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (21.9.06)

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Tel. +49 1805 141538 -01-0806

Table of Contents

Table of Contents

Table of Contents

1 Introduction

The mGuard protects IP data connections. The device supports the following functions:

- Network Card (mGuard PCI), Switch (mGuard delta)
- VPN router (VPN - **V**irtual **P**rivate **N**etwork) for the secure transfer of data via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol)
- Configurable firewall to provide protection against unauthorized access. The dynamic packet filter inspects the source and destination addresses of data packets and blocks undesired traffic.
- Virus protection with support for the protocols HTTP, FTP, SMTP and POP3.

The device can be conveniently configured using a Web browser.

Network features

- Transparent (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (for DSL) and PPTP (for DSL) connectivity
- VLAN
- DHCP server/relay on the external and internal network interfaces
- DNS cache on the internal network interface
- Administration using HTTPS and SSH

Firewall features

- Stateful packet inspection
- Anti-spoofing
- IP Filtering
- L2 Filtering (only Transparent mode)
- NAT with FTP, IRC and PPTP pass through (only router modes)
- 1:1 NAT (only router modes)
- Port forwarding (only router modes)
- Firewall throughput max. 99MBit/s
- Individual firewall rules for different users (user firewall)

Anti-Virus features

- ClamAV virus protection
- Supported protocols: HTTP, FTP, POP3 and SMTP (sending)
- The virus filter can decompress the following formats:
    - ZIP
    - RAR
    - GZIP
    - BZIP2
    - TAR
    - MS OLE2
    - MS Cabinet Dateien (CAB)
    - MS CHM (Komprimiertes HTML)
    - MS SZDD
    - UPX
    - FSG
    - Petite

VPN features

- Protocol: IPsec (Tunnel and Transport Mode)
- IPsec DES encryption - 56 Bit
- IPsec 3DES encryption - 168 Bit
- IPsec AES encryption - 128, 192 and 256 Bit
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with Main and Quick Mode
- Authentication: Pre-Shared Key (PSK), X.509v3 certificate
- DynDNS

- NAT-T
- Dead Peer Detection (DPD)
- Hardware encryption
- up to 250 VPN tunnels (please refer to the feature table)
- VPN throughput max. 35MBits/s on 266MHz or 70MBit/s on 533MHz models.
- IPsec firewall and 1:1 NAT
- Default route over VPN

Additional features

- MAU management
- Remote logging
- Router/Firewall Redundancy
- IPsec/L2TP Server
- LLDP
- Administration by SNMP v1-v3 (please refer to the feature table) and Innominate Device Manager (IDM)

Support

In case of problems with the mGuard please contact your local dealer.
Additional information about the device and relevant changes as well as release notes and software updates can be found on the web site:
- for the EAGLE mGuard under www.hirschmann-ac.com,
- for all other mGuards under http://www.innominate.com/

1.1 Device versions

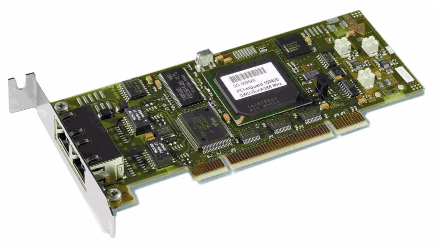
mGuard is available in the following device versions, which have largely identical functions. All devices can be utilised regardless of the processor technology and operating system the connected computers use.

mGuard smart

Smallest device model. Can, for example, simply be plugged between the computer or local network (on mGuard’s LAN port) and an available router (on mGuard’s WAN port), without having to change existing system configurations or driver installations. Designed for instant use in the office or when on the go.

mGuard PCI

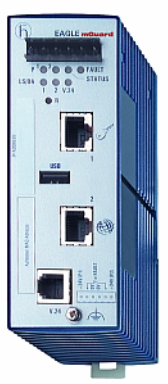
This card, which can be plugged into a PCI slot, provides the computer it is installed in with all mGuard functions in driver mode and can additionally be utilised as a normal network card. A network card already on hand in the computer or another local computer / local network can be connected in the power-over-PCI mode.



mGuard blade

The mGuard blade Pack includes the mGuard bladeBase, which can be easily installed into standard 3 U racks (19 inches) and accommodate up to 12 mGuard blades. Thus this version is ideally suited for use in an industrial environment where it can protect several server systems individually and independently of one another. An additional serial interface enables remote configuration using a telephone dial-up connection or a terminal.

EAGLE mGuard



EAGLE mGuard was developed in co-operation with the Industrial Security Alliance partner Hirschmann Automation and Control GmbH. The device is designed for top hat rail mounting (according to DIN EN 50 022) and is therefore especially suited for use in industrial environments. The optional configuration connection and the option to establish a telephone dial-up connection via the V.24 interface provide for additional applications options.

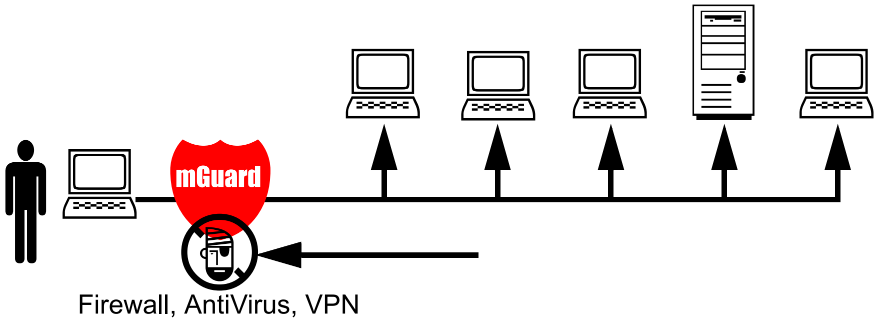
mGuard delta

This device model is a compact LAN switch (Ethernet / Fast Ethernet) designed for connecting up to 4 LAN segments. Thus the device is especially suited for logically segmented network environments where the locally connected computers / networks share the mGuard functions. An additional serial interface enables configuration using a telephone dial-up connection or a terminal. .With its robust metal housing, mGuard delta is not only suitable as a desktop device but also for placement in wiring closets.

2 Typical application scenarios

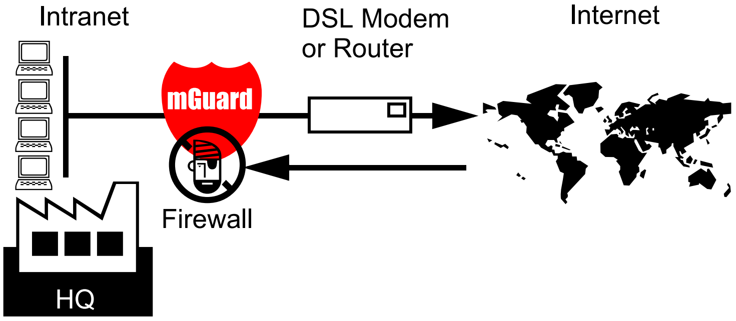
Some of the more common application scenarios may be found below.

Transparent Mode



In *Transparent* Mode (factory default) the mGuard can be installed between an individual computer and the rest of the network.
The settings for Firewall, AntiVirus and VPN can be made with a webbrowser at the URL https://1.1.1.1/.
On the computer itself no configuration changes are required.

Network Router

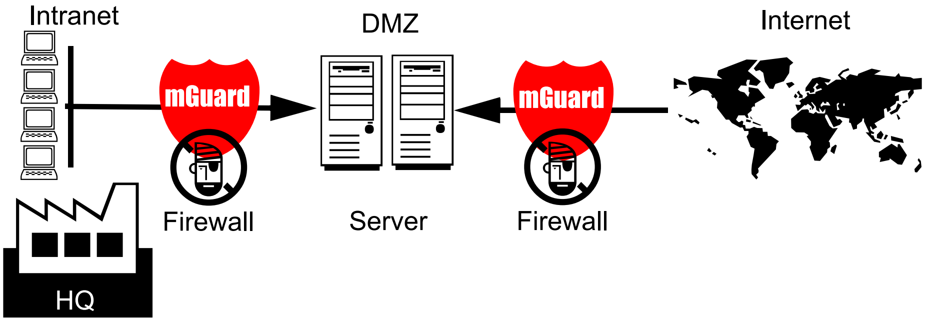


The mGuard is able to provide internet connectivity to a group of computers while protecting the company network with its firewall.
For this purpose one of the following network modes may be used:

- *Router*, if the Internet access is established via a DSL router or dedicated line.
- *PPPoE*, if for example the Internet access is established via a DSL modem using the PPPoE protocol (e.g. in Germany).
- *PPTP*, if for example the Internet access is established via a DSL modem using the PPTP protocol (e.g. in Austria).

The mGuard must be set as the default gateway on the locally connected client system(s).

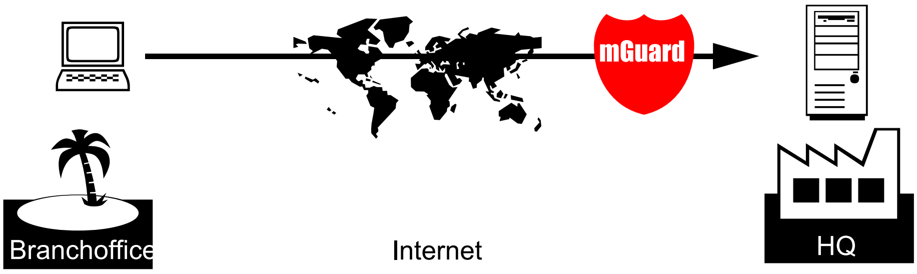
DMZ



A DMZ (Demilitarized Zone) is a protected network, which sits between an tusted network and untrusted networks. For example a company's website may be inside a DMZ, granting FTP write access to computers in the intranet and HTTP read-only access to both networks.
The IP addresses within the DMZ can be public or private. In the latter case, pub-

lic IPs would be mapped by means of portforwarding to the private addresses within the DMZ.

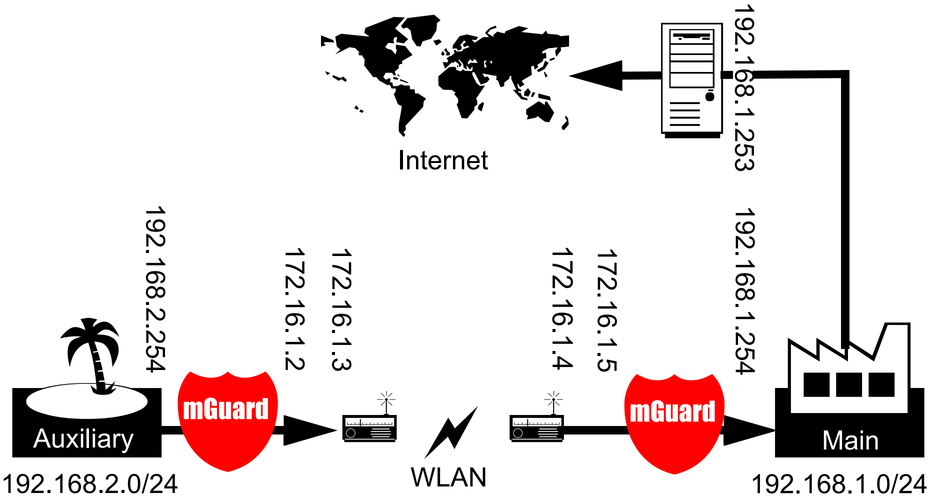
VPN Gateway



An encrypted access to the company's network is to be provided to employees at home or in the field. The mGuard thereby provides the services of a VPN gateway.

On the untrusted computers an IPsec capable VPN client must be installed in case the computers operating system does not provide such a service, like Windows 2000 or XP do.

WLAN over VPN



Two buildings of a company are to be connected with an IPsec protected WLAN connection. From the auxiliary building it shall also be possible to use the main building's internet connection.

In this example the mGuards were switched into router mode and a separate network with addresses of 172.16.1.x was created for the WLAN. Since the internet should be also available via the VPN from the auxiliary building, a "Default route over VPN" must be configured.

Auxiliary building tunnel configuration

Connection type	Tunnel (Net <-> Net)
Local network address	192.168.2.0/24
Remote network address	0.0.0.0/0

In main building the appropriate counterpart to the connection is to be configured:

Main building tunnel configuration

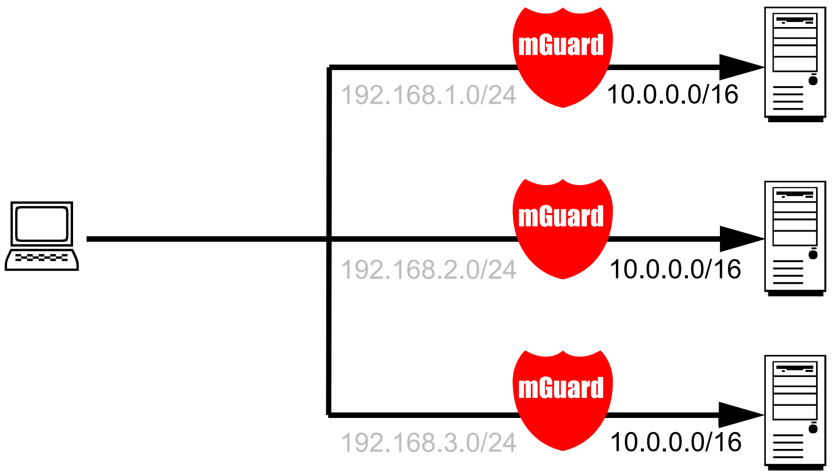
Connection type	Tunnel (Net <-> Net)
Local network address	0.0.0.0/0
Remote network address	192.168.2.0/24

The default route of an mGuard is usually directed over its WAN port. But in this case the internet is reachable via the LAN port:

Main building default gateway

IP of the default gateway	192.168.1.253

Solving Network Conflicts

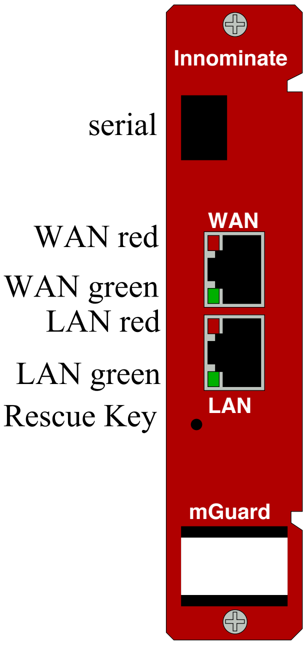


In the illustration above, it is desired that the networks on the right-hand side are accessible from the network or the computer on the left-hand side. For historical or technical reasons, however, the computer networks overlap on the right-hand side.
With the help of mGuards and their 1:1 NAT feature, these networks can be redefined so that the conflict is solved.

(1:1 NAT can be used in normal routing and in IPsec VPN tunnels.)

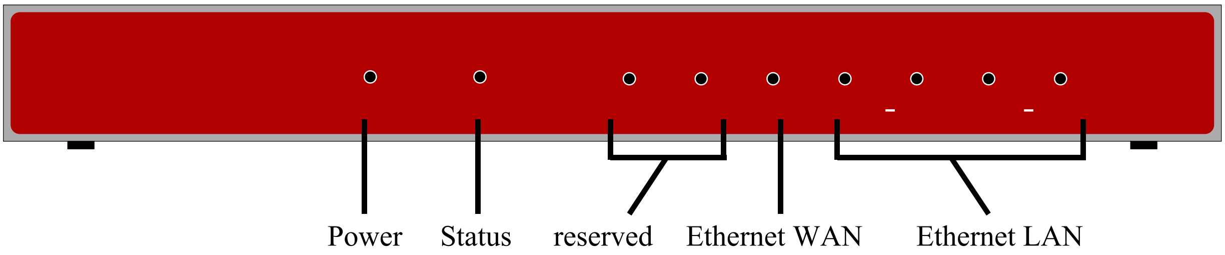
3 Control and LEDs

3.1 mGuard blade



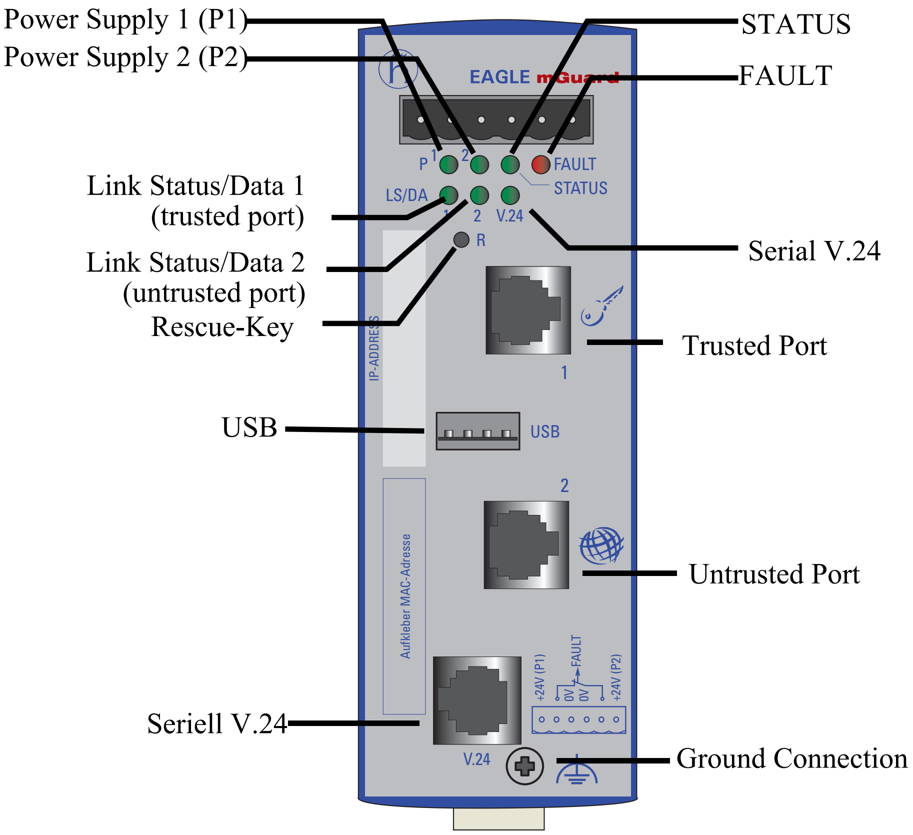
LEDs	State	Meaning
WAN Red, LAN Red	flashing	**Booting up**. After starting or restarting the computer.
WAN Red	flashing	**System error**. ⌧ Perform a system restart. To accomplish this, briefly press the Rescue button (1.5 sec.) If the error occurs again, start the *Recovery procedure* (see "Performing a Recovery" on page 142) or contact Support.
WAN Green, LAN Green	on or flashing	**Ethernet status**. Shows the status of the LAN and WAN interface. As soon as the device is connected to the network, the LEDs will be on continuously to indicate that there is a connection. The LEDs will flash when data packets are transferred.
WAN Green, WAN Red, LAN Green	various LED codes	**Recovery mode**. After pressing the **Rescue key** See "The Rescue Button – restart, recovery procedure and to flash the firmware" on page 142.

3.2 mGuard delta



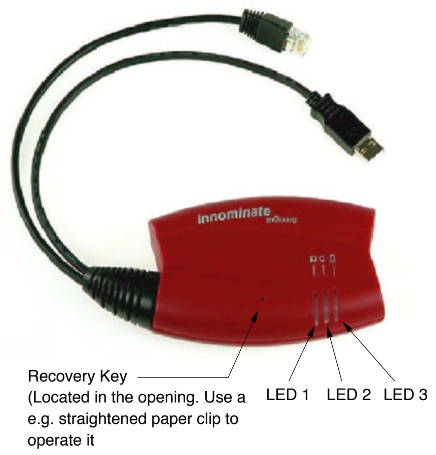
LEDs	State	Meaning
Power	on	The power supply is active.
Status	on	The mGuard is booting.
	heartbeat (flash, flash, pause, ...)	The mGuard is ready.
1,2	-	Reserved.
3 (WAN)	on	Link detected.
	flashing	Data transfer.
4-7 (LAN)	on	Link detected.
	flashing	Data transfer.

3.3 EAGLE mGuard



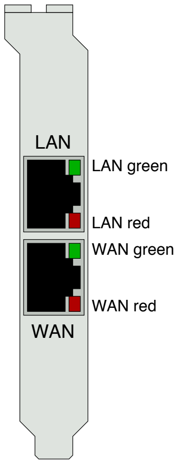
LEDs	State	Meaning
P1, P2	green	The power supply 1 or 2 is active.
STATUS	green blinking	The EAGLE mGuard is booting.
	green	The mGuard is ready.
	yellow blinking slowly	The mGuard is in Router Redundancy Backup mode.
FAULT	red	The signal contact is open in case of an error.
LS/DA 1/2 **V.24**	green	Link detected.
	green blinking (3 times per period)	The port is disabled.
	yellow flashing	Receiving data.
	running light	Initialization phase after a reset.
Display of ACA function STATUS and V.24	both LEDs blinking simultaneously (slow)	ACA writing process.
	both LEDs blinking simultaneously (slow)	ACA reading process.
	both LEDs blinking alternated (fast)	ACA error.

3.4 mGuard smart


Recovery Key
(Located in the opening. Use a
e.g. straightened paper clip to
operate it
LED 1
LED 2
LED 3
innominate
mGuard

LEDs	Colour	State	Meaning
2	Red/Green	red/green flashing	**Booting up**. After connecting the device to the power supply. After a few seconds, the LED will switch to a heartbeat.
	Green	flashing	**Heartbeat**. The device is correctly connected and functioning.
	Red	flashing	**System error**. ⌧ Perform a system restart. To accomplish this, briefly press the **Rescue key** (1.5 sec.) OR Disconnect the device from its power supply briefly and then reconnect it. If the error occurs again, start the *Recovery procedure* (see “Performing a Recovery” on page 142) or contact Support.
1 and **3**	Green	on or flashing	**Ethernet status**. LED 1 shows the status of the internal interface, LED 3 the status of the external interface. As soon as the device is connected to the interface, the LEDs will be on continuously to indicate that there is a connection to the network. The LEDs will flash when data packets are transferred.
1, 2, 3	various LED codes		**Recovery mode**. After pressing the **Rescue key** See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 142.

3.5 mGuard PCI



LEDs	State	Meaning
WAN Red, **LAN Red**	flashing	**Booting up**. After starting or restarting the computer.
WAN Red	flashing	**System error**. ☒ Perform a system restart. To accomplish this, briefly press the **Rescue key** (1.5 sec.) OR Restart your computer. If the error occurs again, start the *Recovery procedure* (see “Performing a Recovery” on page 142) or contact Support.
WAN Green, **LAN Green**	on or flashing	**Ethernet status**. Shows the status of the LAN and WAN interface. As soon as the device is connected to the network, the LEDs will be on continuously to indicate that there is a connection. The LEDs will flash when data packets are transferred.
WAN Green, **WAN Red,** **LAN Green**	various LED codes	**Recovery mode**. After pressing the **Rescue key** See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 142.

4 Startup

Safety instructions

The mGuard is intended for (protective) low voltage operation. Only connect the mGuard's network interfaces to LAN installations. Some telephone lines also use RJ45 jacks. The mGuard may not be operated on a telephone line.

! **Warning mGuard PCI!** Before handling the mGuard PCI, touch the bare metal case of your PC to discharge static electricity from your body.

! **Warning!** This is a Class A device. It may cause radio interference in a living area, in which case, the operator may be requested to take appropriate measures.

General notes regarding usage

- mGuard PCI: Your PC must provide a free PCI slot (3.3V or 5V).
- Use a soft cloth to clean the case of the device. Do not use any aggressive solvents!
- Environmental conditions:
  0 to +40°C (blade, smart) 55°C (PCI) 60° (EAGLE)
  max. 90% (EAGLE: 95%), non-condensing humidity
- To avoid overheating, do not leave it in direct sunlight or expose it to any other source of heat.
- Do not bend the cables sharply. Only use network cables to connect to a network.

Steps for starting up the device

To startup the device, perform the following steps in the order listed:

Step	Objectives	Page
1	Check the package contents and read the Release Notes	"Package contents" on page 18
2	Connect the Device	• "Connect the mGuard blade" on page 19 • "Connect the mGuard delta" on page 21 • "Connect the EAGLE mGuard" on page 22 • "Connect the mGuard smart" on page 24 • "Connect the mGuard PCI" on page 25
3	Configure the device to the extent necessary. To accomplish this, select from the various options offered in the mGuard's configuration menus. For more information regarding which options and settings are required (or desirable) for your operating environment, please read the relevant sections in this manual.	"Local Configuration: At startup" on page 34

4.1 Package contents

Before beginning to setup the device, check that the package is complete:

Included in the package

- a mGuard blade. delta, EAGLE, smart or PCI
- a manual in the Portable Document Format (PDF) on the CD-ROM
- a Quick Installation Guide / Discription and operating instruction

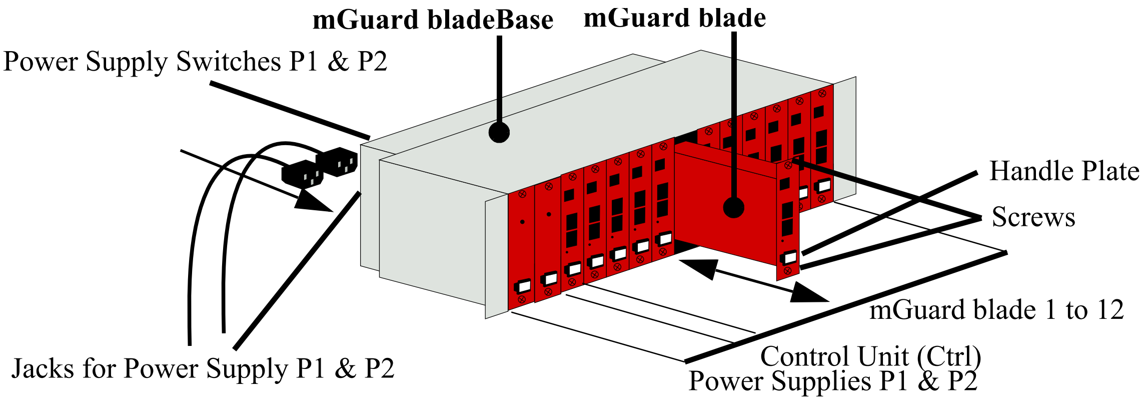
The mGuard bladePack also contains:

- the 19” mguardBlade base
- a mGuard blade as controller
- 2 power supplies
- 2 power cables
- 12 place holders
- 12 handle plates M1 to M12
- screws to install the bladeBase

The mGuard delta also contains:

- the 5V DC power supply
- two UTP ethernet cables
- a RS232 serial cable

4.2 Connect the mGuard blade



Installing mGuard bladeBase

- Install the mGuard bladeBase into the rack, e.g. close to the patch panel.
- Provide the two power supplies and the control unit at their front from the left to the right with the handle plates “P1”, “P2” and “Ctrl”.
- Connect both power supplies on the back of the mGuard bladeBase with 100V or 220/240V.
- Switch both power supplies on.
- The LEDs at the front of the power supplies flash now green.

⌦**It is necessary that a sufficient air circulation through the bladePack is guaranteed!**

⌦**When stacking several bladePacks, one or more 19" rack mount fan trays must be installed to exhaust the accumulated warm air!**

Installing mGuard blade

- Loosen the upper and lower screws of the place holder or mGuard blade you want to replace.
- Remove the place holder or pull the old mGuard blade out of the bladeBase.
- Insert the new mGuard blade with its circuit board into the bladeBase's plastic guidance and push until it is completely inside.
- Secure the mGuard blade by light tightening of the upper and lower screws.
- Replace the empty handle plate with the suitable number from the mGuard bladeBase accessories or the old mGuard blade, by shoving it in or out latteraly.

⌦During installation or removal of an mGuard blade the bladeBase does not need to be switched of.

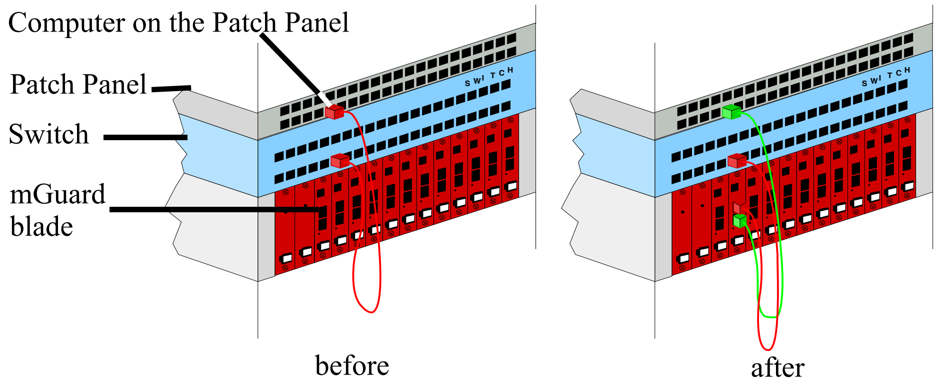
Control Unit (CTRL Slot)

Next to the two current supplies is the “CTRL” Slot. A mGuard blade operated therein works as a controller for all other mGuard blades.

During an mGuard blades first installation into the “CTRL” slot, the blade reconfigures itself into an control unit:

- The web interface is reconfigured to operate as a control unit.
- It switches itself into router mode with the local IP 192.168.1.1.
- The firewall, Anti-Virus and VPN services are reset and deactivated.

Connecting mGuard blade

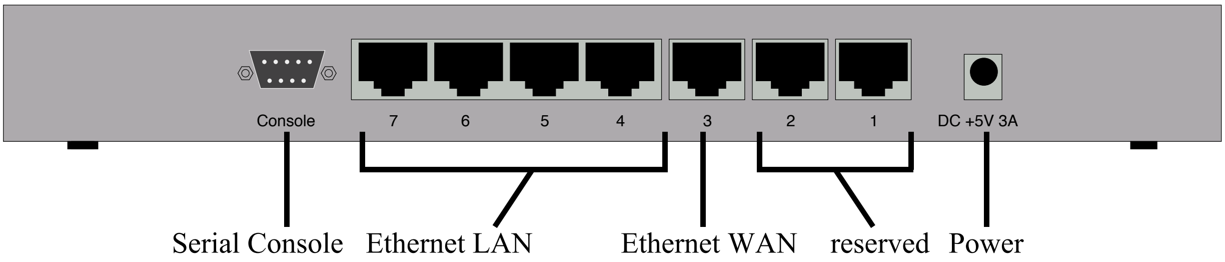


If your computer is already attached to a network, then you just need to patch the mGuard blade between the already existing network connection. Please note that the initial configuration can only be done using the LAN connector and that the firewall is rejecting all IP traffic from the WAN to the LAN interface.

⌦ No additional driver needs to be installed.

⌦ For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration.

4.3 Connect the mGuard delta

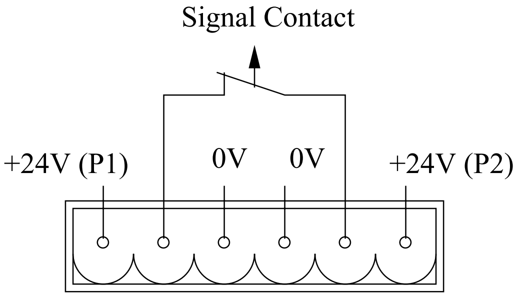


- Connect the power supply (5V DC, 3A) to the mGuard’s power jack.
- Connect the local computer or network to one of the Ethernet LAN jacks (4 to 7) with an UTP (CAT5) ethernet cable.

4.4 Connect the EAGLE mGuard

Terminal block

The **supply voltage** and the **signal contact** are connected via a 6 pin terminal block with snap lock mechanism.



! **Warning!**
The EAGLE mGuard is designed for operation with a safe extra-low voltage.Thus its power supply and signal contact connectors may only be connected with PELV circuits or, alternatively, SELV circuits with voltage restrictions in accordance with IEC/EN 60950.

Operating voltage

NEC Class 2 power source 12VDC or 24 VDC (-25% +33%) safe extra-low voltage (SELV/PELV, redundant inputs decoupled), 5 A maximum. Buffer time min. 10 ms at 24 VDC.

Redundant power supply

Redundant power supplies are supported. Both inputs are decoupled. There is no load distribution. With a redundant supply, only the power pack with the higher output voltage supplies the EAGLE mGuard. The supply voltage is electrically isolated from the housing.

Signal contact

The signal contact is used to supervise the functions of the EAGLE mGuard and thereby facilitates remote diagnosis. An interruption of the potential-free signal contact (relay contact, closed current circuit) indicates the following:

- The failure of at least one of the two supply voltages.
- A permanent fault on the EAGLE mGuard (internal 3.3 V DC voltage, supply voltage 1 or 2 < 9.6 V, ...).
- The faulty link status of at least one port.
  The indication of the link state on the EAGLE mGuard can be masked on a port-by-port basis using the management software.
  State of delivery: there is no link test.
- Self test error.

⌦ In case of a non-redundant voltage supply, the EAGLE mGuard will indicate the failure of the supply voltage. You can correct this by connecting the supply voltage to both inputs.

Ground connection

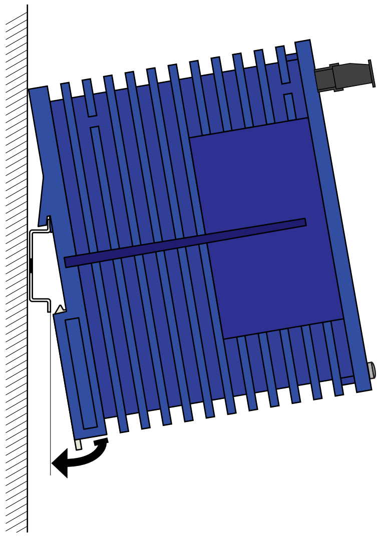
The EAGLE mGuard is grounded with a separate screw connection.

Assembly

The equipment is delivered in a ready-to-operate condition. The following procedure is appropriate for assembly:

- Pull the terminal block off the EAGLE mGuard and wire up the supply voltage and signal contact lines.
- Fit the EAGLE mGuard on a 35 mm standard bar to DIN EN 50 022.

- Attach the upper snap-on slide bar of the EAGLE mGuard to the standard bar and press it down until it locks into position.
- Connect the device to the local network or the local PC which is to be protected (trusted port).
- Connect the socket for connection to the external network (untrusted port), e.g. the Internet. (Via this network the connctions to the remote device or the remote network are realized.)



☒ The front panel of the EAGLE mGuard is grounded via a separate ground connection.

☒ Do not open the housing.

☒ The shielding ground of the twisted pair lines which can be connected is electrically connected to the front panel.

Startup procedure

You do start up the EAGLE mGuard by connecting the supply voltage via the 6-pin terminal block. Lock the terminal block with the snap lock mechanisme.

Network connection

If your computer is already attached to a network, then you just need to patch the EAGLE mGuard between the already existing network connection. Please note that the initial configuration can only be done using the LAN connector and that the firewall is rejecting all IP traffic from the WAN to the LAN interface.

☒ No additional driver needs to be installed.

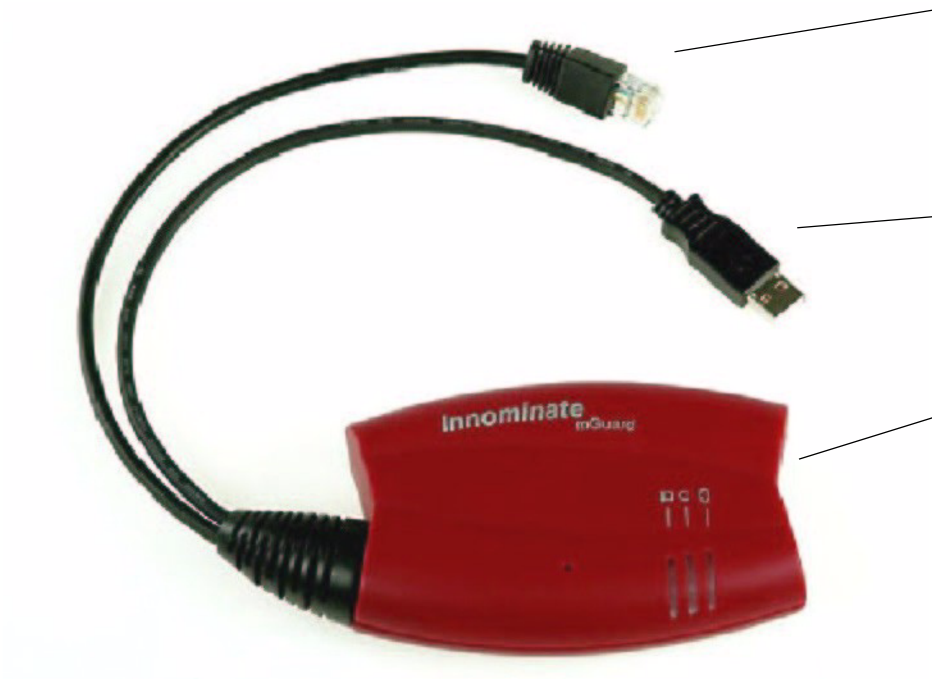
☒ For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration.

☒ Both ports of the EAGLE mGuard are configured to be connected to a computer. If you connect the ports to a hub, please note that if *Autonegotiation* (See “MAU Configuration” on page 64.) is disabled, then the Auto-MDIX will also be deactivated, i.e. the port of the EAGLE mGuard has to be connected either to the uplink port of the hub or a cross-link cable has to be used.

Dismantling

To take the EAGLE mGuard off the ISO/DIN rail, insert a screwdriver horizontally under the housing into the locking slide, pull it (without tipping the screwdriver) downwards and lift the EAGLE mGuard upwards.

4.5 Connect the mGuard smart



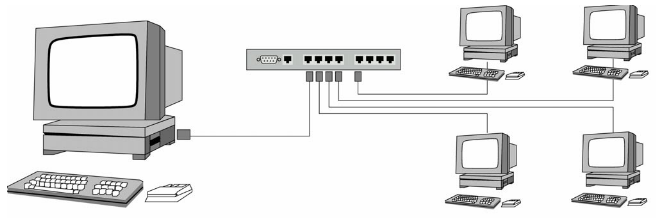
Ethernet plug to connect the unit directly to the system or network to be protected (**local** system or network).

USB connector to connect the unit to a computer's USB interface. Only used to supply power.

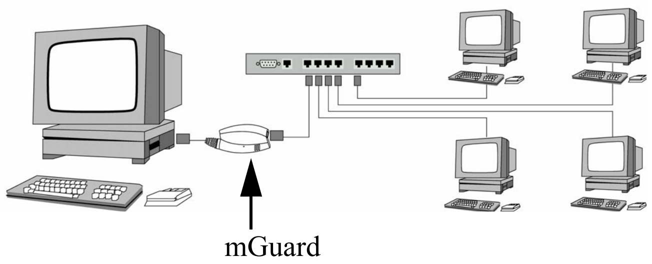
Jack for connecting an external network, e.g. WAN, Internet. (Connections to remote devices or networks are established via this network.)
Use a UTP cable (CAT 5).

If your system is already connected to a network, simply insert the mGuard between the system's network interface and the network.

before:



after:



⌦No additional driver needs to be installed.
⌦For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration.

4.6 Connect the mGuard PCI

4.6.1 Choice between Driver mode or Power-over-PCI mode

There are two operating modes: *Driver mode* or *Power-over-PCI mode*.
The mGuard is switched to operate in the desired mode via a jumper.

Driver mode:
The mGuard PCI can be used like a regular network card, enabling this network card to also provide the mGuard functions. In this case the included driver must be installed.

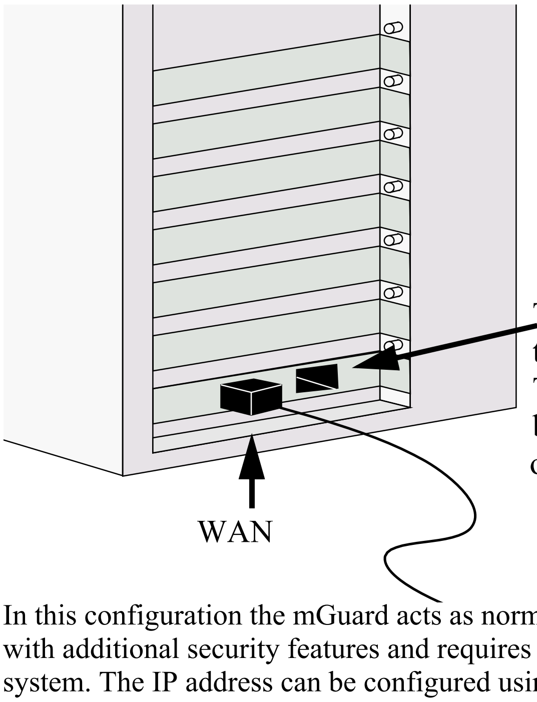
Power-over-PCI mode:
If the mGuard's network card functionality isn't needed or won't be used, then the mGuard PCI can be connected behind an existing network card (of the same computer or of another one), essentially acting as an mGuard standalone device. In this operating mode, in fact, the mGuard PCI is only plugged into the computer's PCI slot to be supplied with power and given a housing. This mGuard operating mode is called *Power-over-PCI mode*. No driver needs to be installed.

Decide in which mode you want the mGuard PCI to operate before installing it on your PC.

Driver Mode

In this mode a driver for the PCI interface of the mGuard PCI (available for Windows XP/2000 and Linux) needs to be installed later on the computer which will provide a “regular” network interface with additional security functions. In Driver Mode an additional network card isn’t needed in the computer.

Transparent Mode with Driver Mode (Factory default)

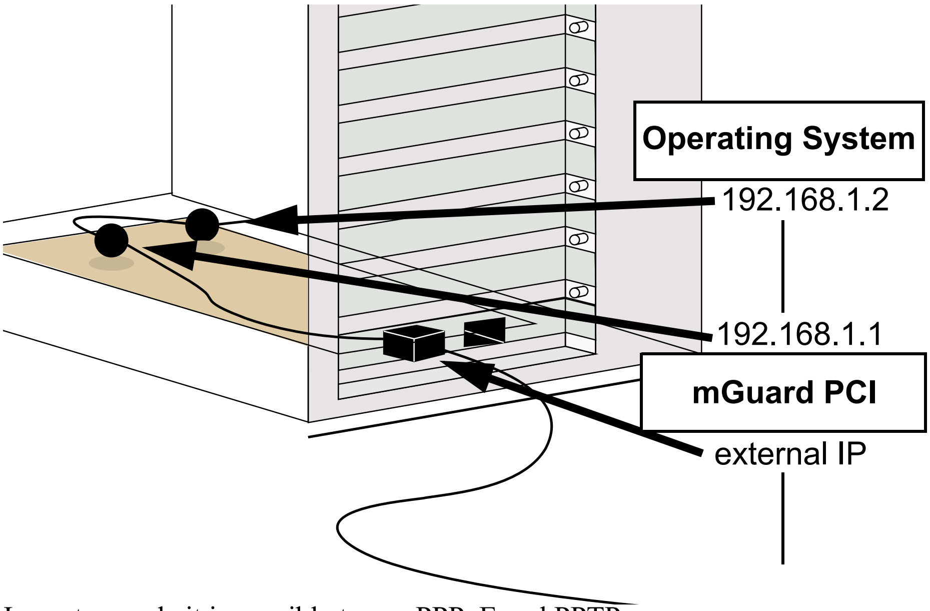


The LAN ethernet jack is deactivated in Driver Mode.
The LAN interface is provided by the driver for the computers operating system.

In this configuration the mGuard acts as normal network interface card (NIC) with additional security features and requires a driver for the host operating system. The IP address can be configured using the network utilities of the operating system.
As soon as an external router is available the mGuard can be configured using a webbrowser at the URL https://1.1.1.1/.

⌦In Transparent Mode it is not possible to use PPPoE or PPTP.

Router Mode with Driver Mode

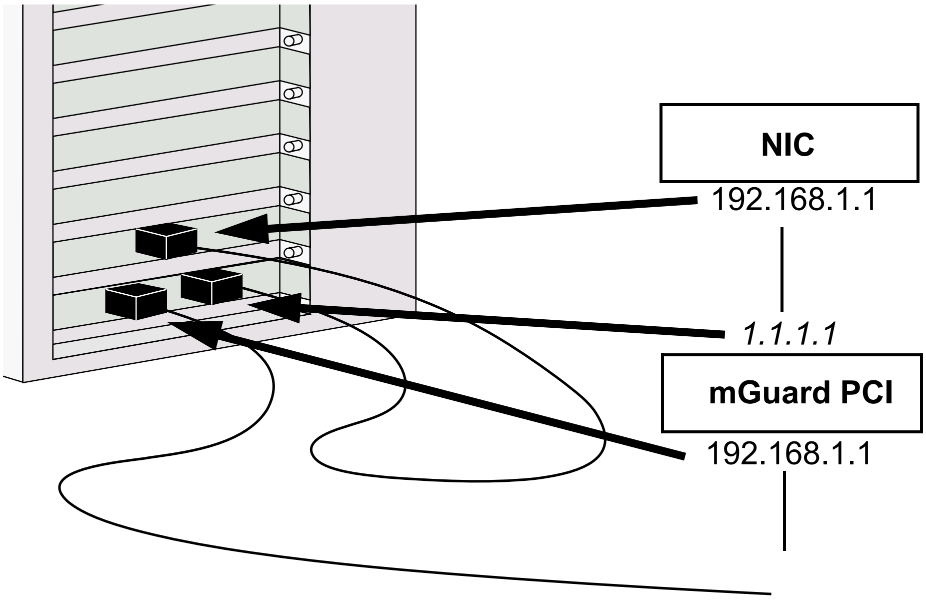


In router mode it is possible to use PPPoE and PPTP.
In this mode the mGuard and the network interface of the mGuard use a separate subnet. An example is shown in the illustration above: the mGuard's operating systems interface could use the IP 192.168.1.1 and the mGuard could use the IP 192.168.1.2. (Represented in the figure above by two black spheres.)
A third IP will be used on the WAN jack to communicate with a router or a PPPoE/PPTP capable DSL modem.

Power-over-PCI Mode

In this mode the software driver is not needed. The PCI interface is only used as a power supply and another network interface card, installed in the same or another computer, must be connected to the ethernet jack (3) instead.

Transparent Mode with Power-over-PCI Mode

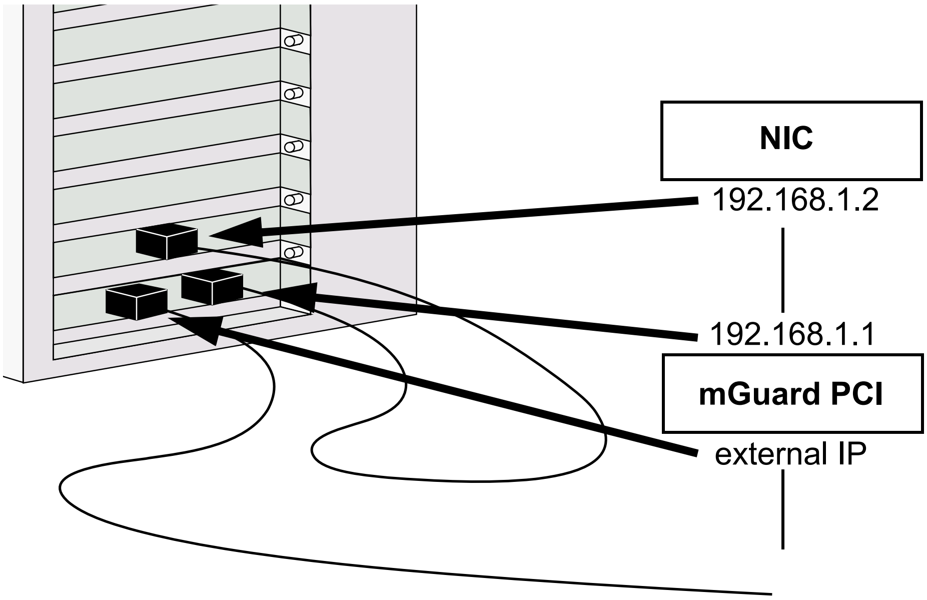


In Power-over-PCI Mode the mGuard does not require a driver for the host operating system. The PCI bus is only used as a power supply. The LAN jack of the mGuard must be connected to another NIC using an ethernet cable. At the WAN jack the mGuard automatically uses the IP address of the other network interface card.
As soon as an external router is available the mGuard can be configured with a

webbrowser at the URL https://1.1.1.1/.

⌦In Transparent Mode its not possible to use PPPoE or PPTP.

Router Mode with Power-over-PCI Mode

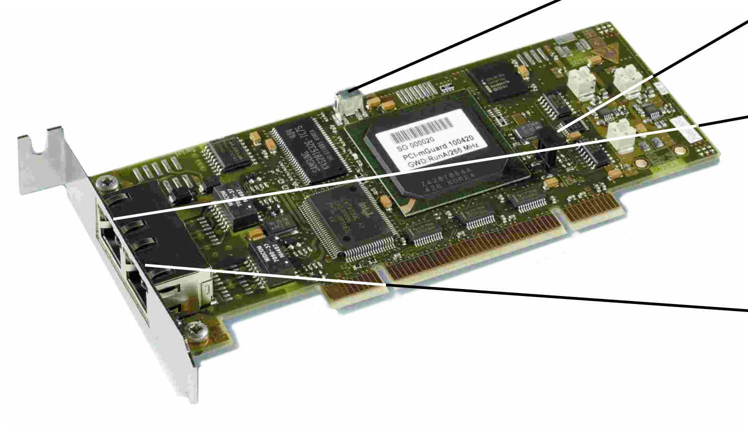


In router mode it is possible to use PPPoE and PPTP.

The mGuard and the network interface card (NIC) connected to the LAN jack use a separate subnet. E.g. the NIC could use the IP 192.168.1.1 and the mGuard’s LAN jack could use the IP 192.168.1.2.

A third IP will be used on the WAN jack to communicate with a router or a PPPoE/PPTP capable DSL modem.

4.6.2 Hardware installation



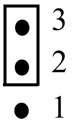
1 Rescue push button

2 Jumper to enable/disable Driver Mode

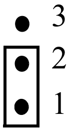
3 Ethernet jack to connect the unit directly to the system or network to be protected (**local** system or network) when Driver Mode is disabled

4 Jack for connecting an external network, e.g. WAN, Internet. (Connections to **remote** devices or networks are established via this network.)
Use a UTP cable (CAT 5).

1. Configure the mGuard for either Driver or Power-over-PCI mode. (See "Choice between Driver mode or Power-over-PCI mode" on page 25.)
   To enable the **Driver Mode**, set the jumper (2) to the following position:

   To enable the **Power-over-PCI Mode**, set jumper (2) to the following position:

2. Turn off the power to your computer and any other connected peripheral devices. Follow the precautions for static electricity discharge.
3. Unplug the power cord from the back of the computer
4. Remove the computer's cover (please consult the manual of your computer).
5. Select a free PCI slot (3.3V or 5V) for the mGuard PCI.
6. Remove the selected slot bracket by unscrewing the holding screw and slide it out. Save this screw for securing the mGuard PCI card after it's installed.
7. To install the PCI card, carefully align the board's bus connector with the selected expansion slot on the motherboard. Push the board down firmly, but gently, until it is well seated.
8. Replace the slot bracket's holding screw to secure the board to the rear slot panel.
9. Put back the computer's cover.
10. Reconnect the power cord and turn on your computer.

4.6.3 Driver installation

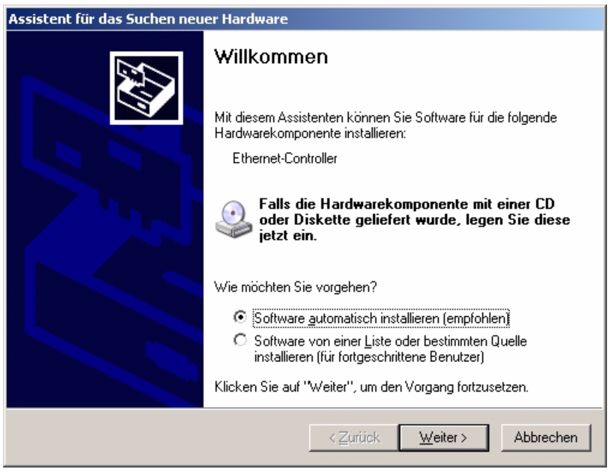
Windows XP

☞ Please complete the steps described in section “Hardware installation” on page 28 first.

⌧ The installation of the driver is only necessary (and will only work as described) in Driver Mode (see “Driver Mode” on page 25).

⌧ The following screen shots show the german version of Windows XP.

To install the driver, switch your computer on, login with Administrator rights and wait for the following window to show up:.



Willkommen

Mit diesem Assistenten können Sie Software für die folgende Hardwarekomponente installieren:

Ethernet-Controller

Falls die Hardwarekomponente mit einer CD oder Diskette geliefert wurde, legen Sie diese jetzt ein.

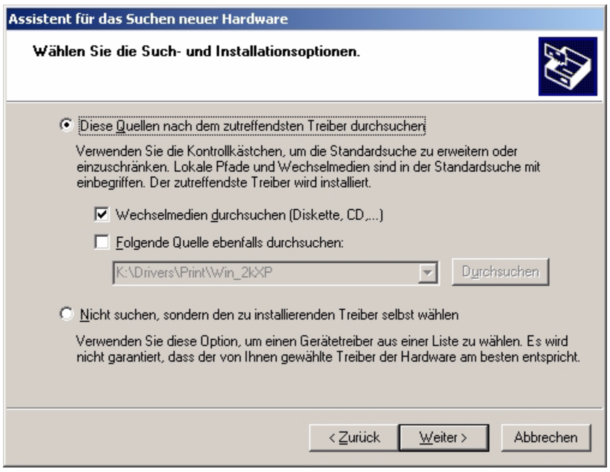
Wie möchten Sie vorgehen?

● Software automatisch installieren (empfohlen)

○ Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

1. After inserting the mGuard-CD choose **From a list or specified location (Advanced)** and click on **Next**



Wählen Sie die Such- und Installationsoptionen.

● Diese Quellen nach dem zutreffendsten Treiber durchsuchen

Verwenden Sie die Kontrollkästchen, um die Standardsuche zu erweitern oder einzuschränken. Lokale Pfade und Wechselmedien sind in der Standardsuche mit einbegriffen. Der zutreffendste Treiber wird installiert.

☑ Wechselmedien durchsuchen (Diskette, CD,...)

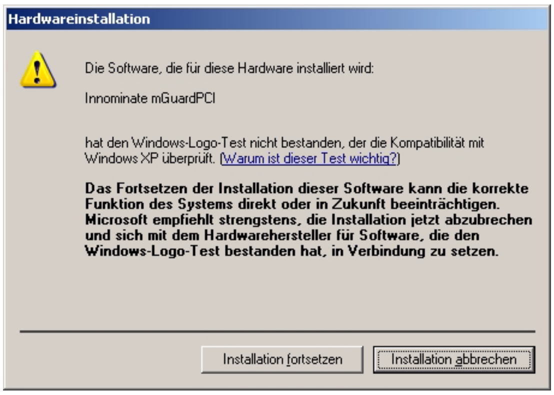
□ Folgende Quelle ebenfalls durchsuchen:

K:\Drivers\Print\Win_2kXP

○ Nicht suchen, sondern den zu installierenden Treiber selbst wählen

Verwenden Sie diese Option, um einen Gerätetreiber aus einer Liste zu wählen. Es wird nicht garantiert, dass der von Ihnen gewählte Treiber der Hardware am besten entspricht.

2. Click on **Next**



Hardwareinstallation

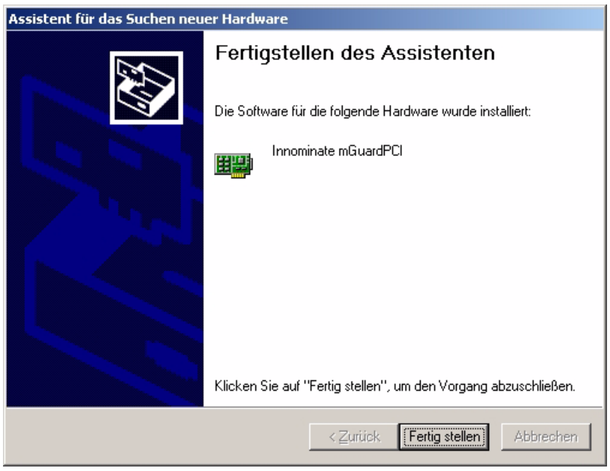
Die Software, die für diese Hardware installiert wird:

Innominate mGuardPCI

hat den Windows-Logo-Test nicht bestanden, der die Kompatibilität mit Windows XP überprüft. (Warum ist dieser Test wichtig?)

Das Fortsetzen der Installation dieser Software kann die korrekte Funktion des Systems direkt oder in Zukunft beeinträchtigen. Microsoft empfiehlt strengstens, die Installation jetzt abzubrechen und sich mit dem Hardwarehersteller für Software, die den Windows-Logo-Test bestanden hat, in Verbindung zu setzen.

3. Click on **Continue anyway**



Assistent für das Suchen neuer Hardware

Fertigstellen des Assistenten

Die Software für die folgende Hardware wurde installiert:

Innominate mGuardPCI

Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.

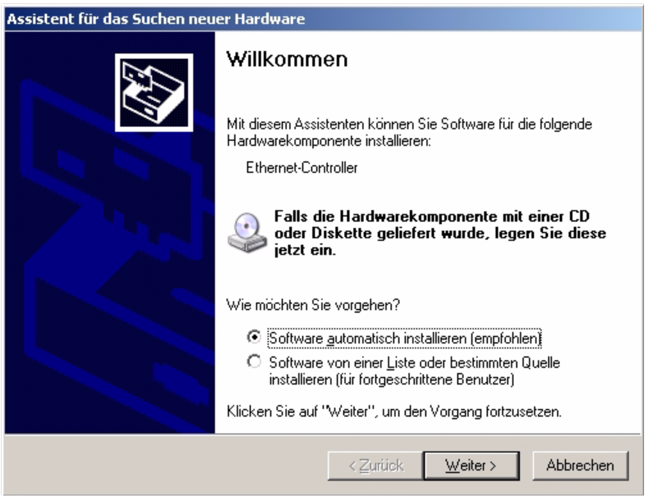
4. Click on **Finish**

Windows 2000

☞ Please complete the steps described in section “Hardware installation” on page 28 first.

⌦ The installation of the driver is only necessary (and will only work as described) in Driver Mode (see “Driver Mode” on page 25)

To install the driver, switch your computer on, login with Administrator rights and wait for the following window to show up:



Assistent für das Suchen neuer Hardware

Willkommen

Mit diesem Assistenten können Sie Software für die folgende Hardwarekomponente installieren:

Ethernet-Controller

Falls die Hardwarekomponente mit einer CD oder Diskette geliefert wurde, legen Sie diese jetzt ein.

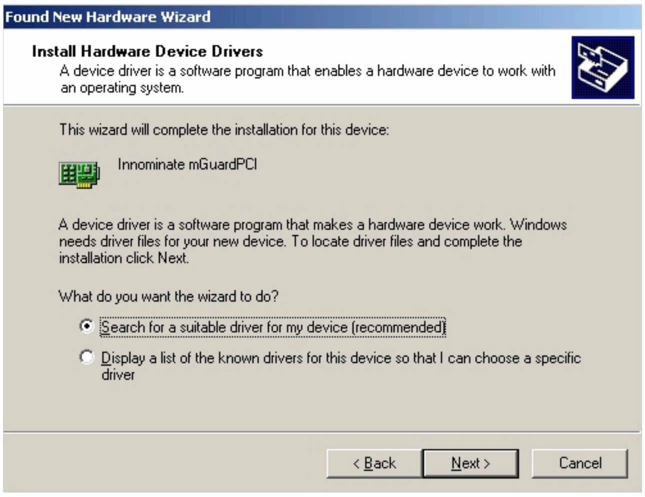
Wie möchten Sie vorgehen?

● Software automatisch installieren (empfohlen)

○ Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

1. Click on **Next**



Found New Hardware Wizard

Install Hardware Device Drivers

A device driver is a software program that enables a hardware device to work with an operating system.

This wizard will complete the installation for this device:

Innominate mGuardPCI

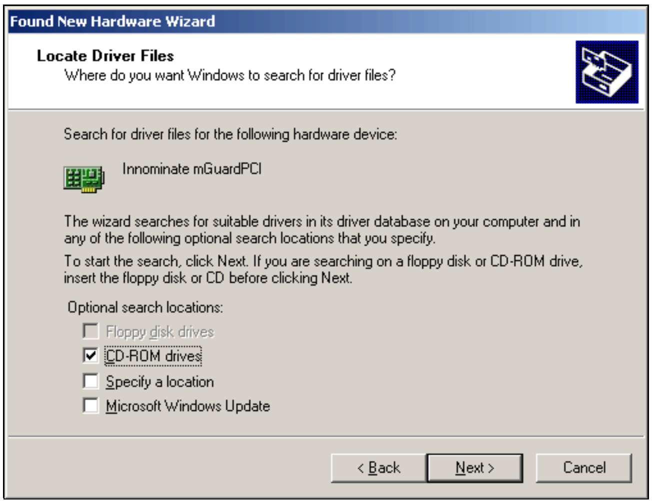
A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.

What do you want the wizard to do?

● Search for a suitable driver for my device (recommended)

○ Display a list of the known drivers for this device so that I can choose a specific driver

2. After inserting the mGuard-CD choose **Search for a suitable driver for my device** and click on **Next**



Found New Hardware Wizard

Locate Driver Files

Where do you want Windows to search for driver files?

Search for driver files for the following hardware device:

Innominate mGuardPCI

The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.

To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.

Optional search locations:

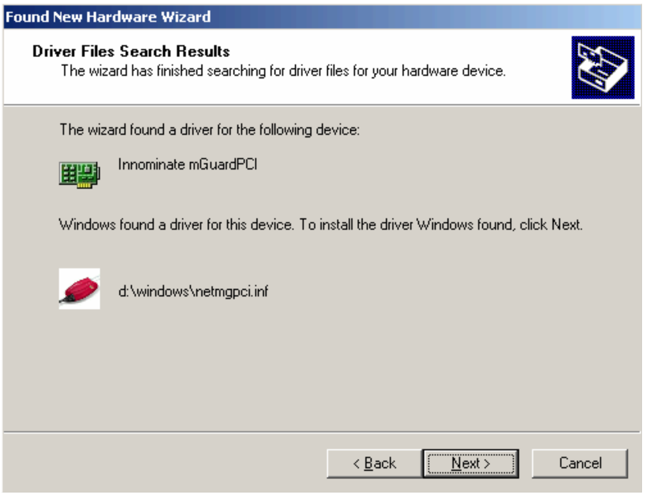
□ Floppy disk drives

☑ CD-ROM drives

□ Specify a location

□ Microsoft Windows Update

3. Select **CD-ROM drives** and click on **Next**


Found New Hardware Wizard

Driver Files Search Results

The wizard has finished searching for driver files for your hardware device.

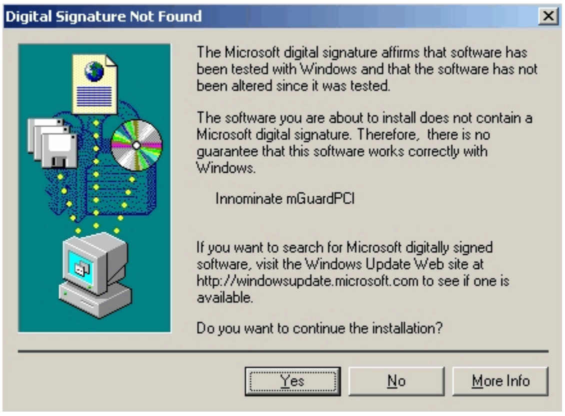
The wizard found a driver for the following device:

Innominate mGuardPCI

Windows found a driver for this device. To install the driver Windows found, click Next.

d:\windows\netmgpci.inf

4. Click on **Next**


Digital Signature Not Found

The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

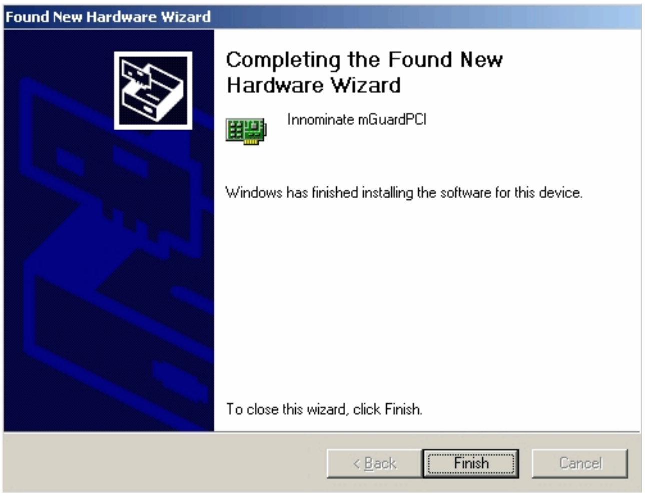
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

Innominate mGuardPCI

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

5. Click on **Yes**


Found New Hardware Wizard

Completing the Found New Hardware Wizard

Innominate mGuardPCI

Windows has finished installing the software for this device.

To close this wizard, click Finish.

6. Click on **Finish**

Linux

The Linux driver is available as a source archive and must be compiled before usage. To do this:

- Build and install the kernel (2.4.26) in **/usr/src/linux**
- Unpack the driver into **/usr/src/pci-driver**
- Issue the following commands in the shell
  - **cd /usr/src/pci-driver**
  - **make LINUXDIR=/usr/src/linux**
  - **install -m0644 mguard.o /lib/modules/2.4.26/kernel/drivers/net/**
  - **depmod -a**
- To load the driver run the following command
  - **modprobe mguard**

5 Configuration preparation

5.1 Connecting the mGuard

mGuard blade

- The mGuard blade must be installed inside the mGuard bladeBase and at least one of the bladeBases power supplies must be on.
- In a local configuration: The system that you use for performing the configuration must either be
  – connected to the LAN jack of the mGuard blade,
  – or connected to it via the local network.
- In the case of a remote configuration: The mGuard must be configured to permit remote configuration.
- The mGuard must be connected, i.e. the required connections must function.

mGuard delta

- The mGuard must be connected to its power supply.
- In a local configuration: The system that you use for performing the configuration must either be
  – connected to the mGuard's LAN switch (ethernet jack 4 to 7)
  – or connected to it via the local network.
- In the case of a remote configuration: The mGuard must be configured to permit remote configuration.
- The mGuard must be connected, i.e. the required connections must function.

EAGLE mGuard

- The EAGLE mGuard must be connected to an active power supply.
- In a local configuration: The system that you use for performing the configuration must either be
  – connected to the trusted port of the EAGLE mGuard,
  – or connected to it via the local network.
- In the case of a remote configuration: The EAGLE mGuard must be configured to permit remote configuration.
- The EAGLE mGuard must be connected, i.e. the required connections must function.

mGuard smart

- The mGuard must be connected to a power-supply. In other words, its USB cable must be connected to a system (or power supply) that is ON.
- In a local configuration: The system that you use for performing the configuration must either be
  – connected to the mGuard's Ethernet plug,
  – or connected to it via the local network.
- In the case of a remote configuration: The mGuard must be configured to permit remote configuration.
- The mGuard must be connected, i.e. the required connections must function.

mGuard PCI

- In a local configuration: The system that you use for performing the configuration must either be
  – equipped with the mGuard drivers when using the Driver Mode or
  – connected to it via the LAN Ethernet connector when using the Power-over-PCI mode.
- In the case of a remote configuration: The mGuard must be configured to permit remote configuration.
- The mGuard must be connected, i.e. the required connections must function.

5.2 Local Configuration: At startup

The mGuard is configured using a Web browser, which is running on the configuration system (e.g. Firefox, MS Internet-Explorer or Safari)
⌦**The Web browser must support SSL (in other words https).**

By default (factory settings), the mGuard is accessible at the following address:

Factory setting:

Transparent Mode: (default setting except mGuard delta)	https://1.1.1.1/
Router Mode: (default setting on mGuard delta)	https://192.168.1.1/

5.2.1 EAGLE mGuard

With a configured network interface

In order for the mGuard to be accessed via the address https://1.1.1.1/, it must of course first be connected to a configured network interface. This is the case, if you insert it into an existing network connection - see the illustration in the section

- "Connect the EAGLE mGuard" on page 22

In this case the Web browser can access the mGuard's configuration interface at the address https://1.1.1.1/ - see "Setting Up a Local Configuration Connection" on page 41. Continue from this point onwards in this case.

Without a configured network interface

If the computer's network interface has not yet been configured

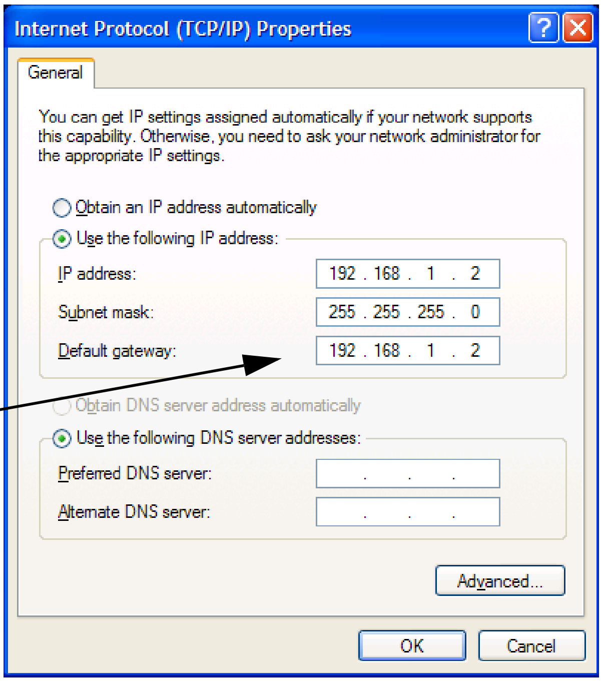
If the system, which will be used to configure the device, was not previously connected to a network, e.g. because the computer is new, its network interface will generally not be configured yet. This means that the system has not yet "been informed" that network traffic should be handled by this interface.

In this case, you must initialize the standard gateway by assigning it a dummy value. To accomplish this, proceed as follows:

Initializing the standard gateway

1. Determine the currently valid standard gateway address.

   If you are using Windows XP, click on **Start, Control Panel, Network Connections**: Right click on the icon of the LAN adapter and then click on **Properties** in the pop-up menu. In the dialog *Internet Protocol Properties* on the *General* tab, select **Internet Protocol (TCP/IP)** under "This connection uses the following items" and then click on the **Properties** button to open the following dialog:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

The IP address of the standard gateway can be examined or set here.

If no IP address has been entered for the standard gateway in this dialog box, e.g. because *Obtain an IP address automatically* has been activated, enter the IP address manually. To do so, first activate **Use the following IP** and then enter, as an example, the following addresses:

IP address:	192.168.1.2
Subnetwork mask:	255.255.255.0
Standard gateway:	192.168.1.1

⌦ Do not under any circumstance assign the configuration system an address like 1.1.1.2!

Entering the IP parameter via HiDiscovery

The HiDiscovery protocol enables you to assign IP parameters to the Switch via the Ethernet.

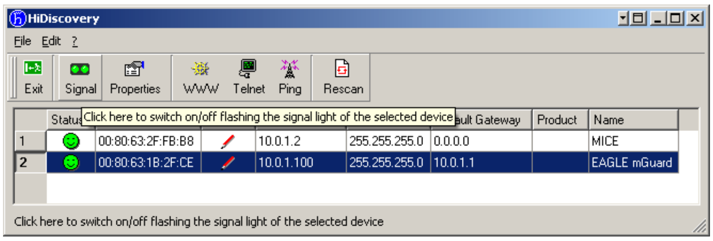
You can easily configure additional parameters with the Web-based management (see “Configuration” on page 44).

Install the HiDiscovery software on your PC. The software is on the CD supplied with the Switch.

1. To install it, you start the installation program on the CD.

⌦ The installation of HiDiscovery involves installing the WinPcap Version 3.0 software package.
If an earlier version of WinPcap is already installed on the PC, then you must first uninstall it. A newer version remains intact when you install HiDiscovery. However, this can not be guaranteed for all future versions of WinPcap. In the event that the installation of HiDiscovery has overwritten a newer version of WinPcap, then you uninstall WinPcap 3.0 and then re-install the new version.

2. Start the HiDiscovery program.



Click here to switch on/off flashing the signal light of the selected device

	Statu					ault Gateway	Product	Name
1	●	00:80:63:2F:FB:B8		10.0.1.2	255.255.255.0	0.0.0.0		MICE
2	●	00:80:63:1B:2F:CE		10.0.1.100	255.255.255.0	10.0.1.1		EAGLE mGuard

Click here to switch on/off flashing the signal light of the selected device

When HiDiscovery is started, it automatically searches the network for those devices which support the HiDiscovery protocol.

HiDiscovery uses the first PC network card found. If your computer has several network cards, you can select these in HiDiscovery on the toolbar.

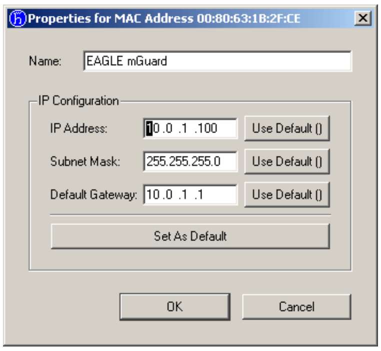
HiDiscovery displays a line for every device which reacts to the HiDiscovery protocol.

⌦ Depending on the protocol in the state of delivery the EAGLE mGuard displays the IP-Address 0.0.0.0 instead of 1.1.1.1.

HiDiscovery enables you to identify the devices displayed.

3. Select a device line.
4. Click on the symbol with the two green dots in the tool bar to set the LEDs for the selected device flashing.
   To Switch off the flashing, click on the symbol again.

By double-clicking a line, you open a window in which you can enter the device name and the IP parameter.



Properties for MAC Address 00:80:63:1B:2F:CE

Name: EAGLE mGuard

IP Configuration

IP Address: 10 .0 .1 .100

Subnet Mask: 255.255.255.0

Default Gateway: 10 .0 .1 .1

☒ After the IP address has been entered, the Switch loads the local configuration settings. Save the settings you have made so they will still be available after restart (see “Basic Settings → Load/Save” on page 65).

☒ For security reasons, Switch off the HiDiscovery function for the device in the Web-based interface, after you have assigned the IP parameters to the device (see “Basic Settings → System” on page 46).

5.2.2 mGuard blade and mGuard smart

With a configured network interface

In order for the mGuard to be accessed via the address https://1.1.1.1/, it must of course first be connected to a configured network interface. This is the case, if you insert it into an existing network connection - see the illustration in the section

- “Connect the mGuard blade” on page 19
- “Connect the mGuard smart” on page 24.

In this case the Web browser can access the mGuard's configuration interface at the address https://1.1.1.1/ - see “Setting Up a Local Configuration Connection” on page 41. Continue from this point onwards in this case.

Without a configured network interface

If the computer’s network interface has not yet been configured

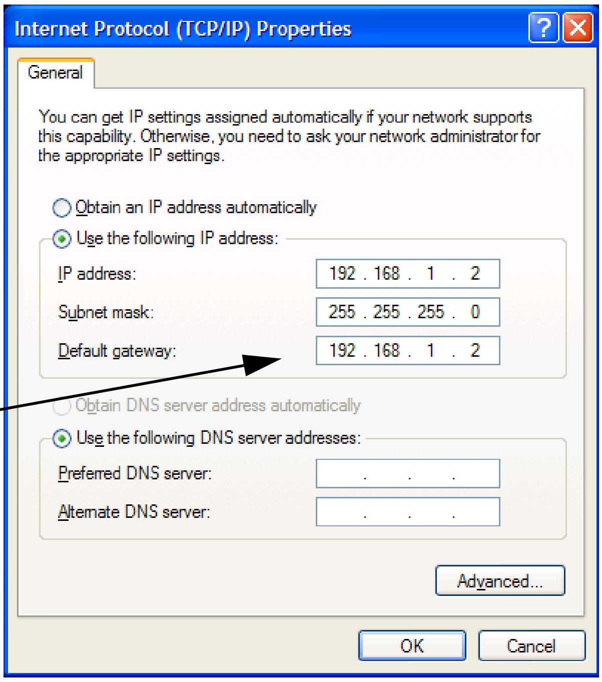
If the system, which will be used to configure the device, was not previously connected to a network, e.g. because the computer is new, its network interface will generally not be configured yet. This means that the system has not yet “been informed” that network traffic should be handled by this interface.

In this case, you must initialize the standard gateway by assigning it a dummy value. To accomplish this, proceed as follows:

Initializing the standard gateway

1. Determine the currently valid standard gateway address.

   If you are using Windows XP, click on **Start, Control Panel, Network Connections**: Right click on the icon of the LAN adapter and then click on **Properties** in the pop-up menu. In the dialog *Internet Protocol Properties* on the *General* tab, select **Internet Protocol (TCP/IP)** under “This connection uses the following items” and then click on the **Properties** button to open the following dialog:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

The IP address of the standard gateway can be examined or set here.

If no IP address has been entered for the standard gateway in this dialog box, e.g. because *Obtain an IP address automatically* has been activated, enter the IP address manually. To do so, first activate **Use the following IP** and then enter, as an example, the following addresses:

IP address:	192.168.1.2
Subnetwork mask:	255.255.255.0
Standard gateway:	192.168.1.1

⌧ Do not under any circumstance assign the configuration system an address like 1.1.1.2!

2. On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter:

   `arp -s` <IP of the standard gateway> **`aa-aa-aa-aa-aa-aa`**

   Example:

   You have determined that the address of the standard gateway is [or you have set it to]: 192.168.1.1

   Then the command should be:

   ```
   arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa
   ```

3. To proceed with the configuration, first establish the necessary connection - see “Setting Up a Local Configuration Connection” on page 41.

4. After setting the configuration, restore the original setting for the standard gateway address. To do so, either restart the configuration computer or enter the following command at the DOS level [in the Command Prompt window]:

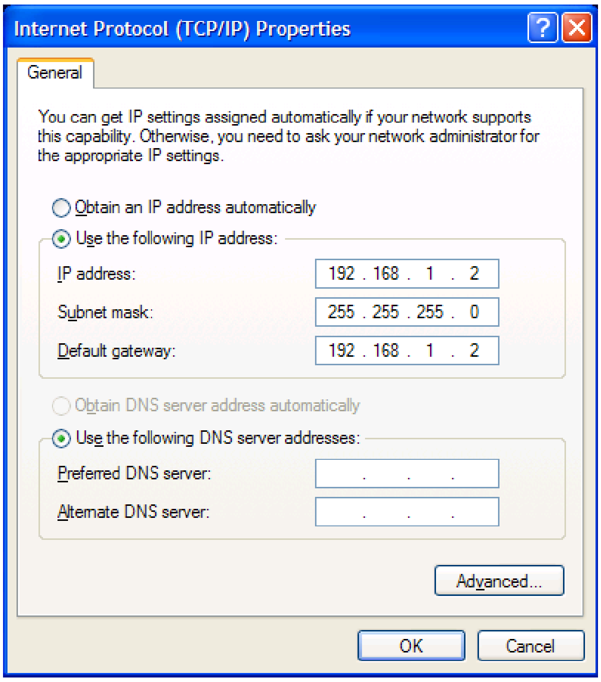
   ```
   arp -d
   ```

5.2.3 mGuard delta

The mGuard delta’s initial IP address on the LAN interfaces 4 to 7 is 192.168.1.1 within the network 192.168.1.0/24 and you may need to adjust the configuration off your computer to access it.

If you are using Windows XP, click on **Start, Control Panel, Network Connections**:

- Right click on the icon of the LAN adapter and then
- click on **Properties** in the pop-up menu.
- In the dialog *Internet Protocol Properties* on the *General* tab, select **Internet Protocol (TCP/IP)** under "This connection uses the following items" and then
- click on the **Properties** button to open the following dialog:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Activate **Use the following IP** and then enter the following address:

IP address:	192.168.1.2
Subnetwork mask:	255.255.255.0
Standard gateway:	192.168.1.1

⌧ Depending on how you configure the mGuard, you may also need to modify the network interface settings of the locally connected system or network accordingly.

5.2.4 mGuard PCI

Install the mGuard PCI Card

When you haven't already installed the mGuard PCI card in your computer, please follow the steps as described in "Hardware installation" on page 28.

Install the mGuard PCI Driver

When you've configured the mGuard to run in Driver Mode, make sure that you've installed the drivers as described in "Driver installation" on page 29.

Configure the Network Interface

If you

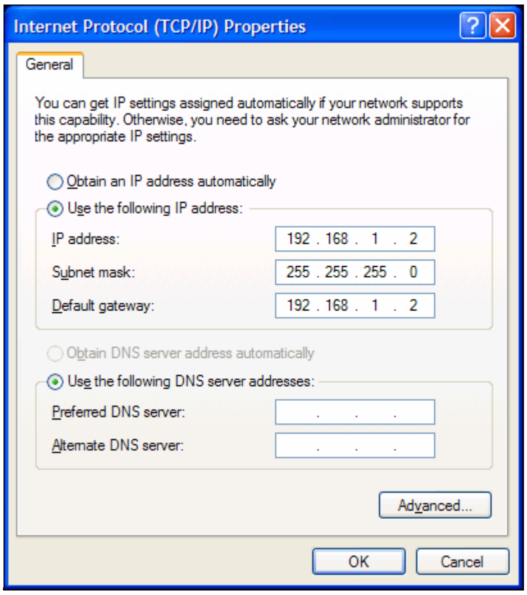
• operate mGuard in the driver mode and the LAN interface (= computer's network interface) has not yet been configured

OR

• operate mGuard in the Power-over-PCI mode and the computer's network interface, which is connected to mGuard's LAN interface, has not yet been configured, this network interface must be configured before you can configure mGuard.

If you are using Windows XP:

- – Click on **Start, Control Panel, Network Connections**
- – Right click on the icon of the LAN adapter
- – Click on **Properties** in the pop-up menu.
- – In the dialog *Internet Protocol Properties* on the *General* tab, select **Internet Protocol (TCP/IP)** under “This connection uses the following items”
- – Click on the **Properties** button to open the dialog you see to the right.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 2

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

The Default Gateway

After you’ve configured the network interface, you should be able to access the mGuard’s configuration interface with a Web browser at the URL “https://1.1.1.1/”. In case this isn’t possible, then your computers default gateway might not be available and you must initialize the standard gateway by assigning it a dummy value. To accomplish this, proceed as follows:

Initializing the standard gateway

1. Determine the currently valid standard gateway address. If you are using Windows XP, follow the steps described above under “Configure the Network Interface” to open the **Internet Protocol (TCP/IP) Properties** dialog box.

   If no IP address has been entered for the default gateway in this dialog box, e.g. because *Obtain an IP address automatically* has been activated, enter the IP address manually. To do so, first activate **Use the following IP** and then enter, as an example, the following addresses:

IP address:	192.168.1.2
Subnetwork mask:	255.255.255.0
Standard gateway:	192.168.1.1

☒ Do not under any circumstance assign the configuration system an address like 1.1.1.2!

2. On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter:

```
arp  -s  <IP of the default gateway>  aa-aa-aa-aa-aa-aa
```

   Example:

   You have determined that the address of the default gateway is [or you have set it to]: 192.168.1.1

   Then the command should be:

```
arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa
```

3. You should now be able to access the mGuard’s configuration interface at the URL https://1.1.1.1/. Please see “Setting Up a Local Configuration Connection” on page 41 for full details.
4. After setting the configuration, restore the original setting for the standard gateway address. To do so, either restart the configuration computer or enter the following command at the DOS level [in the Command Prompt window]:

```
arp -d
```

⌦Depending on how you configure the mGuard, you may also need to modify the network interface settings of the host operating system or locally connected system accordingly.

5.3 Setting Up a Local Configuration Connection

Web-based Administrator interface

The mGuard is configured using a Web browser, which is running on the configuration system (e.g. Firefox since version 1.5, MS Internet-Explorer since version 5.0, Safari oder w3m.)

⌦**The Web browser must support SSL (in other words https).**

Depending on the mGuard’s network mode (= mode of operation), it can be accessed (with the factory settings) at one of the following addresses:

Factory setting:

Transparent Mode (default setting):	https://1.1.1.1/
Router / PPPoE / PPPT Mode:	https://192.168.1.1/

Proceed as follows:

1. Start a Web browser.
   (For example, Firefox, MS Internet Explorer or Safari; the Web browser must support SSL (i.e. https).)
2. Make certain that the browser does not automatically dialup a connection when it is started because this could make it more difficult to establish a connection to the mGuard.
   In MS Internet Explorer, you can prevent this with the following setting: In the **Extras menu, select Internet Options...** and click on the *Connections*: tab.
   Make certain that *Never dial a connection* is selected under **Dial-up and Virtual Private Network settings**.
3. Enter the complete address of the mGuard into the browser’s address field.
   In **Transparent** mode (= factory setting except mGuard delta) this address always is

```
https://1.1.1.1/
```

and in **Router** (= factory setting on mGuard delta), **PPPoE** or **PPTP** mode, the factory setting for the mGuard's address is

```
https://192.168.1.1/
```

The mGuard's default IP address in *Transparent* mode:
https://1.1.1.1/
and not in *Transparent* mode:
https://192.168.1.1/

Afterwards:

the mGuard’s Administrator Web page will be displayed. The security notice shown under “After a connection has been successfully setup” on page 42 will displayed.

⌧ If you have forgotten the configured address:

If the address of the mGuard – in *Router*, *PPPoE* or *PPTP* mode – has been changed to a different value and you do not know the device's current address, you must use the **Rescue** key to restore it to factory default. (see "Performing a Recovery" on page 142).

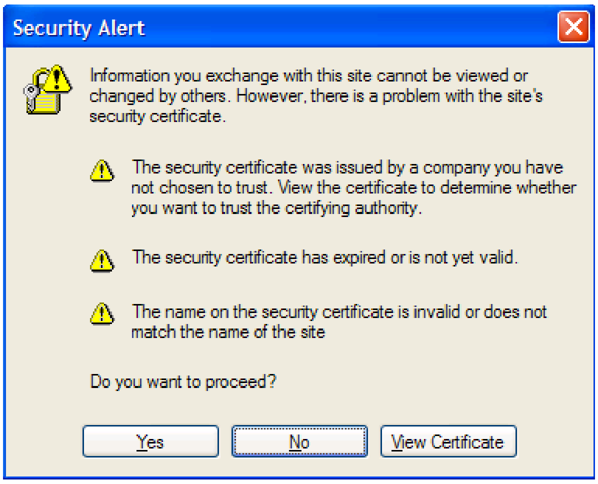
⌧ If the Administrator Web page is not displayed...

If – even after repeated attempts – the Web browser still reports that the page cannot be displayed, try the following:

- Check whether the standard gateway has been initialized on the connected configuration system. See "Local Configuration: At startup" on page 34
- Try disabling any existing firewall.
- Make certain that the browser does not use a proxy server.
  In MS Internet Explorer (Version 6.0), you can prevent this with the following setting: In the **Extras menu, select Internet Options...** and click on the *Connections*: tab. Under *LAN Settings* click on the **Properties...** button and, in the *Local Area Network (LAN) Settings* dialog, check to make certain that **Use a proxy server for your LAN** (under Proxy server) is not activated.
- If any other LAN connection is active on the system, deactivate it until the configuration has been completed.
  Under the Windows **Start menu, Settings, Control Panel, Network Connections** or **Network and Dial-up Connections**, right click on the associated icon and select **Disable** in the pop-up menu.

After a connection has been successfully setup

After the connection has been successfully setup, the following security notice will be displayed (MS Internet Explorer):


Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate has expired or is not yet valid.

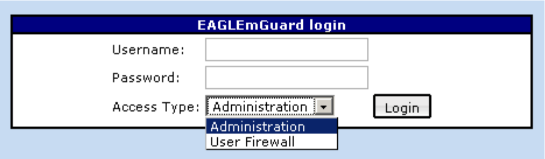
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Explanation:
Since administrative tasks can only be performed when a secure (encrypted) access has been established to the device, a signed (by the device) certificate will be returned.

Acknowledge the associated security notice by clicking on **Yes**.

Afterwards:
The login window is displayed:


EAGLEmGuard login

Username:

Password:

Access Type: Administration

Choose the Access Type — Administration or User Firewall — and enter your username and password for this access type. (Please see “Network Security → User Firewall” on page 95 for an explanation of the User Firewall.)

The factory settings for the Administration are:

Device	**mGuard smart** **mGuard PCI** **mGuard blade** **mGuard delta**	**EAGLE mGuard**
Login:	**admin**	**`admin`**
Password:	**mGuard**	**`private`**

⌦ Please note, these entries are case-sensitive!

To configure the device, proceed as follows:

Configuring the device

1. Select the page with the desired configuration options from the menu - see Page 44.
2. Make the desired settings on the associated page.
3. Once you have confirmed the changes by clicking on **OK**, the new settings will be activated on the device.
   The system will display a confirming message.

If the changes are not shown when you open the page again, because the browser has loaded the page from a cache, reload the page to refresh the display. To do so, click on the appropriate icon in the browser toolbar.

⌦ Depending on how you configure the mGuard, you may also need to modify the network interface settings of the locally connected system or network accordingly.

5.4 Remote Configuration

Prerequisite

The mGuard must be configured to permit remote configuration.

⌦ For reasons of security, remote configuration is disabled by default.

For information on how to enable remote configuration, see section “Security → Web Access” on page 79.

Remote configuration

To configure the mGuard from a remote computer, first establish a connection between it and the local mGuard.
Proceed as follows:

1. Start a Web browser (e.g. Firefox, MS Internet Explorer or Safari; the Web browser must support SSL (i.e. https)).
2. As the address, enter “https://” followed by the IP address or hostname under which the mGuard can be reached.

   Example:
   If this mGuard can be found in the Internet at the address 123.456.789.21 and the Port Number 443 has been set as the port for remote access, you must enter the following address in the Web browser’s address field on the remote system: https://123.456.789.21/. If a different Port Number is used, this must be appended to the IP address, e. g.: https://123.456.789.21:442/

6 Configuration

6.1 Operation

Screen Layout

1. Via the left-hand menu, click on the page with the desired setting possibilities, e.g. *Administration -> Licensing*. The page will then be displayed in the main window - in the form of a register card - on which you can define the settings. If necessary, the page will be organized into several register cards. You may browse through these cards using the tabs at the top.
2. On the relevant page or register card, make the desired entries. To do so, see also the subsection “What happens if inadmissible values are entered” on page 44.
3. In order to adopt the settings, click on the **Apply** button.. After the data has been saved by the system, you will receive a confirmation message. This indicates that the new settings have come into effect. They will also remain valid following restart (reset).

What happens if inadmissible values are entered

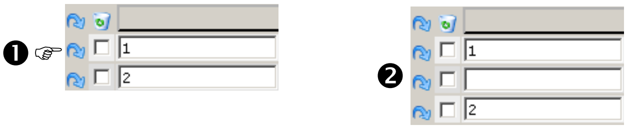
After inadmissible values are entered (for example, an inadmissible number in an IP address) and after subsequently clicking Apply, the letters of the relevant tab card titles will be displayed in red. This helps you in tracking down the error.

Working with tables

Many settings are saved as data records. Correspondingly, the adjustable parameters and their values are presented in the form of table rows. If settings have been created for several data records (e.g. firewall rules), these will be queried or processed based on the sequence of entries from top to bottom. Therefore, if applicable, it is important to pay attention to the order of the entries. By shifting table rows either up or down, the order can be changed.

With tables, you can
- insert rows in order to set up a new data record with settings (e.g. the firewall rules for a specific connection)
- move rows (i.e. shift them to another location) and
- delete rows, in order to delete the entire data record.

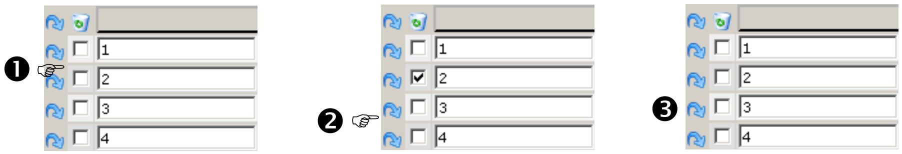
Insert row



1. Click on the arrow under which you want to insert a new row:

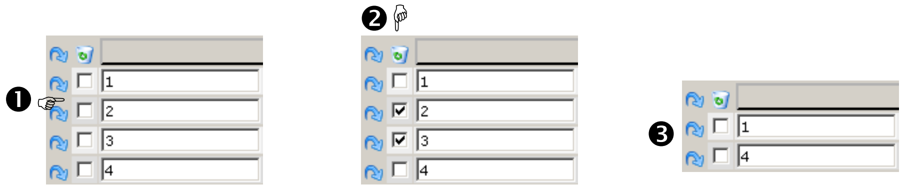
2. Result: The new row is inserted.

Move rows



1. Mark one or more rows you want to move.
2. Click on the arrow under which you want to move the marked rows:
3. Result: The rows are moved.

Delete rows



1. Mark the rows you want to delete.
2. Click on the symbol to delete the rows:
3. Result: The rows are deleted.

Further operating remarks

⌧ If the browser is reloading a page from the cache and therefore displaying an earlier version, you may update the page display to the latest version. To do so, click the update symbol in the browser toolbar.

The following buttons are located in every page header on the mGuards smart, blade,PCI amd delta:

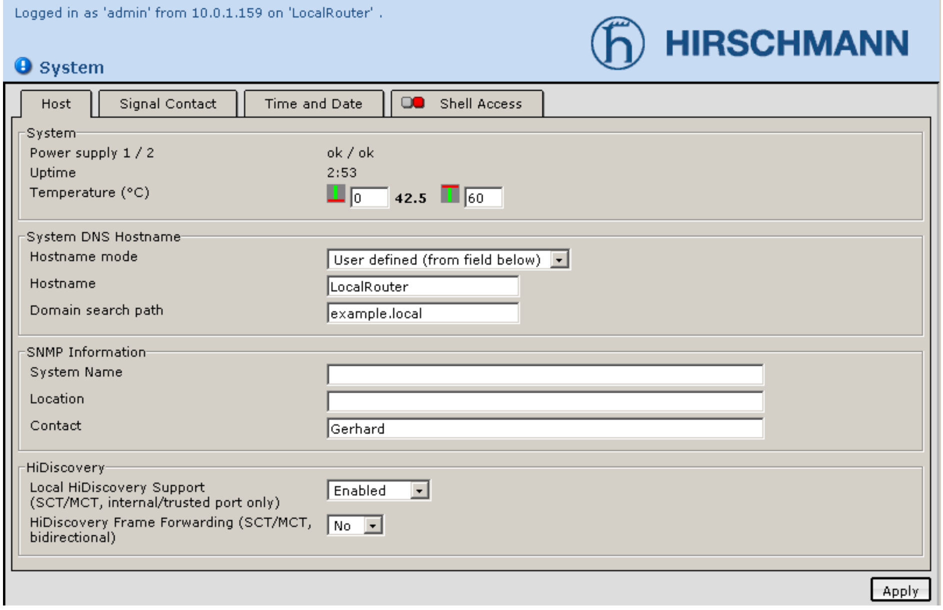
Logout	For logging out after configuration access to the mGuard. If the user does not conduct a logout procedure, the logout is automatically conducted if no more activity takes place and the timeout has expired. Renewed access is only granted after the login process has been repeated.
Reset	Optional button. Resets data to the previous values. If you have entered values on a configuration page and these haven't yet been applied, you can restore the previous values on the page by clicking the **Reset** button. This button is only included in the page header if the validity range of the **Apply** button is set to *include all pages* - see "Security → Web Access" on page 79.
Apply	Optional button. Functions similar to the **Apply** button (see above) but is valid for all pages. This button is only included in the page header if the validity range of the **Apply** button is set to *include all pages* - see "Security → Web Access" on page 79.

6.2 Menu Basic Settings

⌧For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration - see “Passwords” on page 81. As long as the passwords have not been changed, you will see a notice at the top of the page.

6.2.1 *Basic Settings → System*

Host



Logged in as 'admin' from 10.0.1.159 on 'LocalRouter' .

System

System
Power supply 1 / 2: ok / ok
Uptime: 2:53
Temperature (°C): 0 42.5 60

System DNS Hostname
Hostname mode: User defined (from field below)
Hostname: LocalRouter
Domain search path: example.local

SNMP Information
System Name:
Location:
Contact: Gerhard

HiDiscovery
Local HiDiscovery Support (SCT/MCT, internal/trusted port only): Enabled
HiDiscovery Frame Forwarding (SCT/MCT, bidirectional): No

System (only EAGLE mGuard)

Power supply 1/2

The state of both power supplies.

Uptime

The system uptime since the last reboot.

Temperature (°C)

If the temperature exceeds the specified range a SNMP trap is sent.

System DNS Hostname

Hostname mode

Using the *Hostname mode* and *Hostname* fields, you can assign a name to the mGuard. This will then be displayed, e.g. when logging in via SSH. The administration of multiple mGuards is simplified if you assign hostnames to them.

User defined (see below)

(Default) The name entered in the *Hostname* field is assigned to the mGuard.

☞ If the mGuard is running in *Transparent* mode, the option *User defined* must be selected under *Hostname mode*.

Provider defined (e.g. via DHCP)

If the selected network mode permits the external setting of the hostname e.g. via DHCP, the name received from the provider will be assigned to the mGuard.

Hostname

If the option *User defined* is selected under *Hostname mode*, enter the name which should be assigned to the mGuard here.

Otherwise, i.e. if the option *Provider defined (e.g. via DHCP)* is selected under *Hostname mode*, the entry in this field will be ignored.

Domain search path

This entry makes it easier for the user to specify a domain name: If the user enters the domain name in an abbreviated form, the mGuard will extend the entry by appending the domain suffix, which is defined here in the *Domain search path*.

SNMP Information

Systemname

An informational name for the mGuard, eg. “Hermes”, “Pluto”.
(sysName under SNMP)

Location

The physical location of this mGuard.
(sysLocation under SNMP)

Contact

The name of the contact person for this mGuard, together with information on how to contact this person.
(sysContact under SNMP)

Rack ID (only mGuard blade)

The ID of the rack in which the mGuard is installed. On the controller this value can be changed.

Slot ID (only mGuard blade)

The ID of the slot in which the mGuard is installed. Either “Ctrl” or a number between 1 and 12.

HiDiscovery

HiDiscovery is a protocol which supports the initial start-up of new network devices and is activated in the mGuard's *Transparent* mode on the mGuard’s LAN port.

☞ HiDiscovery can be accessed from the trusted network only.

☞ The mGuard must be operated in the Transparent mode.

Local HiDiscovery Support

Activated

The HiDiscovery protocol is activated.

Read only

The HiDiscovery protocol is activated, but the mGuard cannot be configured through it.

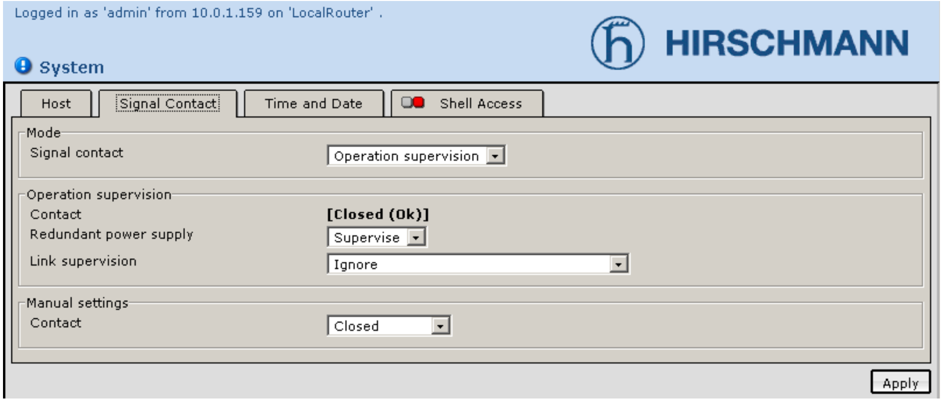
Deactivated

The HiDiscovery protocol is deactivated.

HiDiscovery Frame Forwarding

If this option is activated, then HiDiscovery frames are forwarded from the trusted port via the untrusted port.

Signal contact (only EAGLE mGuard)



Logged in as 'admin' from 10.0.1.159 on 'LocalRouter' .

System

Mode

Signal contact: Operation supervision

Operation supervision

Contact: [Closed (Ok)]

Redundant power supply: Supervise

Link supervision: Ignore

Manual settings

Contact: Closed

The signal contact is a relais which is used by the mGuard to signal error conditions. (See “Signal contact” on page 22.)

Mode

Signal contact

The signal contact can be controlled by the mGuard through automatic **Operation supervision** or **Manual setting**.

Operation supervision

Contact

Displays the state of the the signal contact. Either **Open (Error)** oder **Closed (Ok)**.

Redundant power supply

If set to **Ignore**, the power supply doesn’t influence the signal contact. If set to **Supervise**, the signal contact will be opened when one of the power supplies fails or during permanent malfunction inside the mGuard (internal voltage of 3,3 VDC, power supply < 9,6V, ...).

Link supervision

Supervision of the ethernet interfaces link state. Possible settings are:

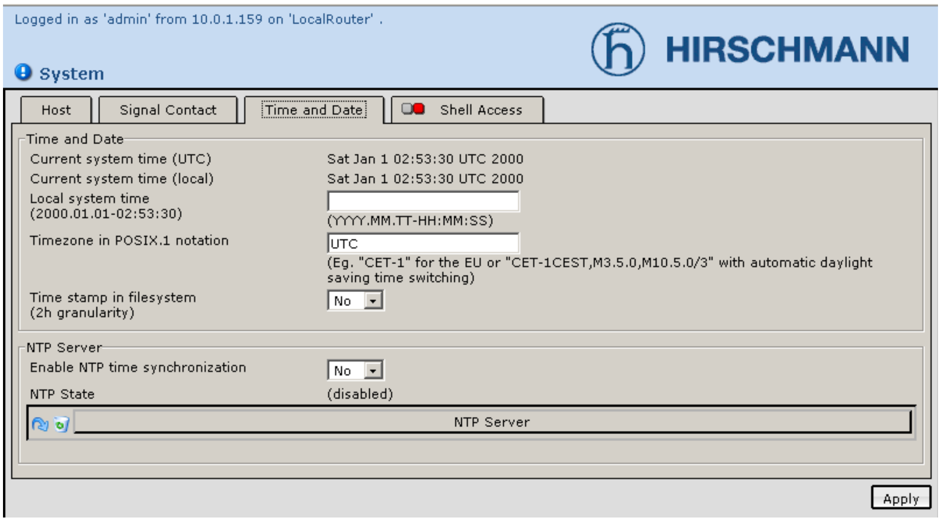
- Ignore
- Supervise only trusted port
- Supervise only unntrusted port
- Supervise both ports

Manual settings

Contact

If the signal contact is set to **Manual setting**, this option sets the contact to **Closed** or **Open (Alarm)**.

Time and Date



Logged in as 'admin' from 10.0.1.159 on 'LocalRouter' .

System

Host | Signal Contact | Time and Date | Shell Access

Time and Date

Current system time (UTC) Sat Jan 1 02:53:30 UTC 2000

Current system time (local) Sat Jan 1 02:53:30 UTC 2000

Local system time (2000.01.01-02:53:30) (YYYY.MM.TT-HH:MM:SS)

Timezone in POSIX.1 notation UTC

(Eg. "CET-1" for the EU or "CET-1CEST,M3.5.0,M10.5.0/3" with automatic daylight saving time switching)

Time stamp in filesystem (2h granularity) No

NTP Server

Enable NTP time synchronization No

NTP State (disabled)

NTP Server

Apply

Time and Date

Current system time (UTC)

Displays the current system time in Universal Time Coordinates (UTC). If the *Enable NTP time synchronisation* is not yet activated (see below) and *Time stamp in filesystem* is deactivated, the clock will start with 1 January 2000.

Current system time (local)

If the possibly differing current local time should be displayed, you must make the corresponding entry under *Timezone in POSIX.1 notation...* (see below).

Local system time

Here you can set the mGuard's in case no NTP server has been specified or the NTP server isn't reachable.

The date and time are specified in the format YYYY.MM.DD-hh:mm:

YYYY	Year
MM	Month
DD	Day
hh	Hour
mm	Minute

Timezone in POSIX.1 notation...

If the Current *system time* above should display your current local time instead of the current time (if it is different to the Greenwich Mean Time), you must enter the number of hours (plus or minus) that your local time differs from Greenwich Mean Time.

Examples:

In Germany, the time is one hour earlier than in Greenwich. Therefore, enter: CET-1.

In New York the clock is behind by hours relative to Greenwich Mean Time. So you enter: GMT+5. The only important thing is the value -1, -2 or +1 etc., because only this will be evaluated – the preceding letters won't be. They can be substituted with "CET" or any other designation, such as "UTC".

If you wish to display Central European Time (for example for Germany) and have it automatically switch to/from daylight saving time, enter: CET-1CEST,M3.5.0,M10.5.0/3

Time stamp in filesystem (2hr granularity): Yes / No

If this option is set to **Yes**, the mGuard will save the current system time to its memory every two hours.

Afterwards: If the mGuard is switched off and back on, a time from this two hour period of time will be displayed when the mGuard is switched on and not (the factory setting) a time on 1 January 2000.

NTP Server

Enable NTP time synchronisation Yes / No

Once the NTP is enabled, the mGuard takes the time from the Internet and displays this as its current system time. The synchronisation can take several seconds.

If this option is set to **Yes** and at least one time server is specified under *NTP servers to synchronize to* (see below), the current system time will be retrieved over the internet.

NTP State

Displays the current NTP state

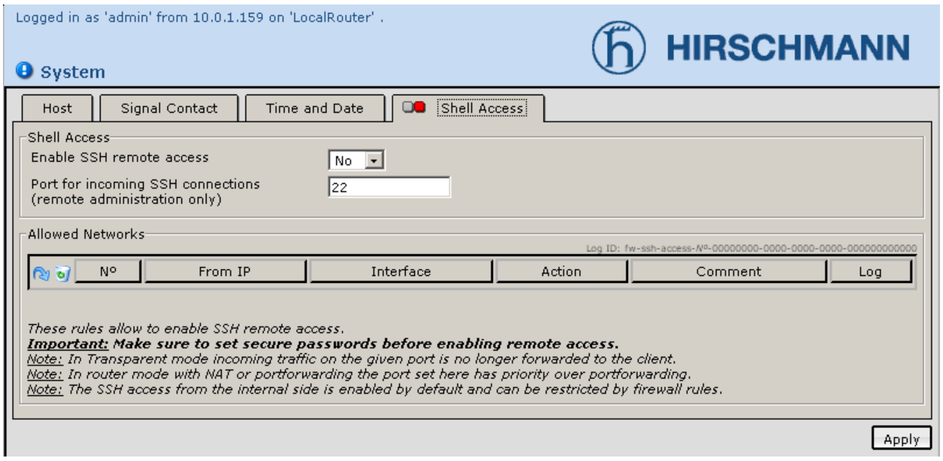
NTP server

Enter one or more time servers from which the mGuard should obtain the current time. If you enter multiple time servers, the mGuard will automatically connect with all of them to determine the current time.

☞ If you enter a hostname, e.g. pool.ntp.org, instead of an IP address, a DNS server must also be specified - see “Log → Settings” on page 126.

☞ If the mGuard is operating in *Router*, *PPPoE* or *PPTP* mode, it will also make the NTP time available to the locally connected systems.

Shell Access



Logged in as 'admin' from 10.0.1.159 on 'LocalRouter' .

Shell Access

Enable SSH remote access: No

Port for incoming SSH connections (remote administration only): 22

Allowed Networks

Log ID: fw-ssh-access-Nº-00000000-0000-0000-0000-000000000000

Nº	From IP	Interface	Action	Comment	Log

These rules allow to enable SSH remote access.

***Important:* Make sure to set secure passwords before enabling remote access.**

Note: In Transparent mode incoming traffic on the given port is no longer forwarded to the client.

Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.

Note: The SSH access from the internal side is enabled by default and can be restricted by firewall rules.

Shell Access

When SSH Remote Access is enabled the mGuard can be configured from a remote system using the command line interface.

This option is disabled by default.

IMPORTANT:If you enable remote access, make certain that you have secure root and administrator passwords.

To enable SSH Remote Access, proceed as follows:

Enable SSH remote access: Yes / No

If you want to allow SSH connections, set this switch to **Yes**.

☞ In this case, make certain that the firewall rules on this page permit the mGuard be accessed from a remote site.

Port for incoming SSH connections (remote administration only)

Standard: 22

You can select a different port.

Example:

If this mGuard can be found in the Internet at the address 123.456.789.21 and the Port Number 22 has been set as the port for remote access, you may need not enter this port number in the address field on the remote system's SSH client.

If a different port number has been set (e.g. 22222), this must be specified to the SSH client, e.g.:

ssh -p 22222 123.456.789.21

Allowed Networks

Lists the firewall rules that have been set. These apply for the incoming data packets of an SSH remote access.

You can define (further more) rules.

From IP

Enter the address(es) of the system(s) that is/are allowed remote access in this field.

You have the following options for the entries:

- IP address: **0.0.0.0/0** means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

Interface

Trusted OR **Untrusted**

Defines for which interface the rule applies, the trusted port or the untrusted port.

State on delivery: the untrusted port discards all, the trusted port accepts all.

Action

Possible settings:

- Accept
- Reject
- Drop

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, *Reject* has the same effect as *Drop*.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

☞ In Transparent mode, *Reject* is not supported.

Comment

An informational comment for this rule.

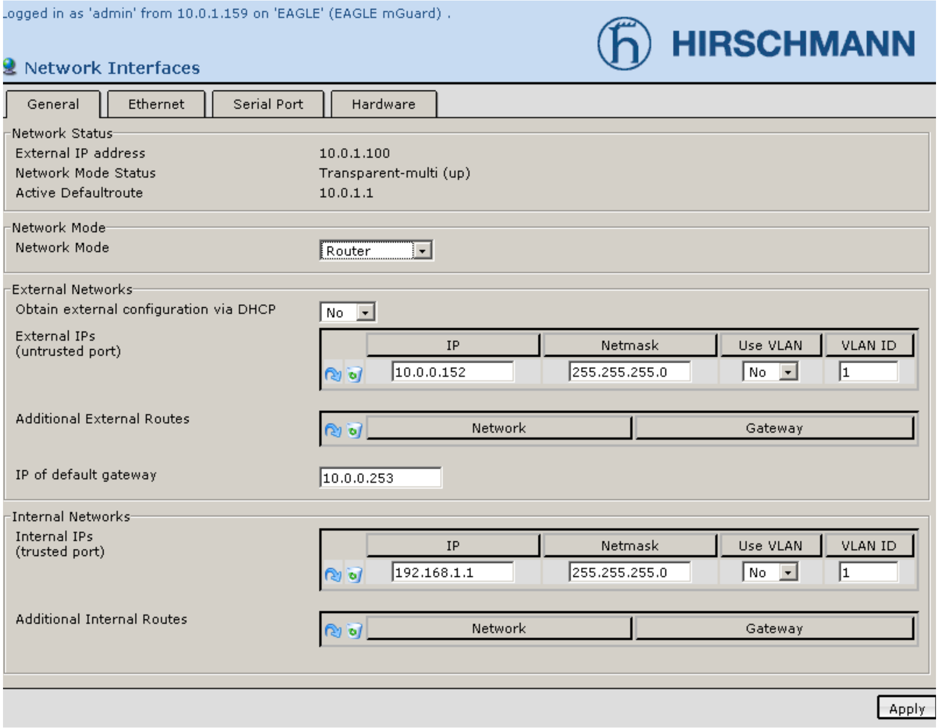
Log

You can specify - for each individual firewall rule - whether the use of the rule

- should be logged by setting - *Log* to **Yes**
- or should not be logged by setting - *Log* to **No** (factory setting).

6.2.2 Basic Settings → Network Interfaces

General



ogged in as 'admin' from 10.0.1.159 on 'EAGLE' (EAGLE mGuard) .

Network Interfaces

Network Status

External IP address	10.0.1.100
Network Mode Status	Transparent-multi (up)
Active Defaultroute	10.0.1.1

Network Mode

Network Mode: Router

External Networks

Obtain external configuration via DHCP: No

External IPs (untrusted port)

IP	Netmask	Use VLAN	VLAN ID
10.0.0.152	255.255.255.0	No	1

Additional External Routes

Network	Gateway

IP of default gateway: 10.0.0.253

Internal Networks

Internal IPs (trusted port)

IP	Netmask	Use VLAN	VLAN ID
192.168.1.1	255.255.255.0	No	1

Additional Internal Routes

Network	Gateway

Network Status

External IP address – WAN port address

Display only: The addresses through which mGuard can be accessed by devices from the external network. They form the interface to other parts of the LAN or to the Internet. If the transition to the Internet takes place here, the IP addresses are usually designated by the Internet Service Provider (ISP). If mGuard is assigned an IP address dynamically, you can look up the currently valid IP address here.

In *Transparent mode*, mGuard adopts the address of the connected local computer as its external IP.

Network mode status

Displays the status of the selected network mode.

Active default route

The IP address that mGuard uses to try to reach networks unknown to it is displayed here. If mGuard is in Transparent mode or if the IP address that is specified as the standard gateway in the connected computer's configuration is not correct, (none) is shown here.

Network mode

The mGuard has to be set to the network mode that corresponds to its local computer or network connection, respectively. See "Typical application scenarios" on page 11

☞ Depending to which Network Mode the mGuard is set, the page is also modified using the configuration parameters defined for it:

- **Transparent** *(factory setting (except mGuard delta))*

  Transparent mode is only used when a single computer is locally connected to the device as a client.

  In this mode, the device can be simply integrated (inserted) into an existing network connection of the respective computer. In this case, simply insert the mGuard into the network line - see the illustration in the section “Connect the mGuard smart” on page 24.

  The mGuard will analyze the network traffic passing through it and configure its network connection accordingly. It will then operate transparently, i.e. without requiring that the client be reconfigured.

  As in the other modes, the mGuard supports the Firewall, Anti Virus and in Single Transparent mode VPN security functions.

  DHCP data (received from outside) will be passed through to the connected client.

  ☞ In case a firewall is installed on the client, it must be configured to allow ICMP Echo Requests (ping). Otherwise the mGuard won’t be able to use services like VPN, DNS, NTP, etc.

  ☞ In Transparent mode the mGuard uses 1.1.1.1 as its internal IP address which is accessible when the client’s configured default gateway is also accessible.

- **Router** *(factory setting (mGuard delta))*

  If the mGuard is not in *Transparent* mode, it serves as a gateway between different networks and has both an external and an internal IP address.

  External Interface (= untrusted port):

  The external interface (WAN) of the mGuard is connected to the Internet or other parts of the LAN.

  - mGuard smart: the ethernet jack

  Internal Interface (= trusted port):

  A network or a single system is connected to its internal interface (LAN):

  - mGuard smart: the Ethernet plug
  - mGuard PCI: The internal interface is in Driver Mode the network interface of the Operating System or in Power-over-PCI mode the LAN Ethernet jack of the mGuard PCI.

  As in the other cases, the mGuard supports the Firewall and VPN security functions in this mode of operation as well.

  ☞ If the mGuard is operated in *Router* mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the mGuard. See “Initializing the standard gateway” on page 37.

  ☞ If the mGuard is operated in *Router* mode and is used to establish the connection to the Internet, you should activate NAT to allow access to the Internet from the local network - see “Network Address Translation/ IP Masquerading” on page 90. If NAT is not activated, the device may only allow VPN connections.

- **PPPoE**

  PPPoE mode corresponds to the Router mode with DHCP – with one difference: The PPPoE protocol, which is used by many DSL modems (for DSL Internet access), will be used, - as it is in Germany, for connecting to the external network (Internet or WAN). The external IP address, under which the mGuard can be reached from a remote site, is assigned by the Internet Service Provider.

☞ If the mGuard is operated in *PPPoE* mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the mGuard. See “Initializing the standard gateway” on page 37.

☞ If the mGuard is in *PPPoE* mode, NAT must be activated to enable access to the Internet - see “Network Address Translation/IP Masquerading” on page 90. If NAT is not activated, the device will only allow VPN connections.

- **PPTP**
  This mode is similar to *PPPoE* mode. In Austria, for example, PPTP is used instead of the PPPoE protocol for DSL connections.
  (PPTP is the protocol, which was originally used by Microsoft for VPN connections.)

  ☞ If the mGuard is operated in *PPTP* mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the mGuard. See “Initializing the standard gateway” on page 37.

  ☞ If the mGuard is operated in *PPTP* mode, you should activate NAT to allow access to the Internet from the local network - see “Network Address Translation/IP Masquerading” on page 90. If NAT is not activated, the device will only allow VPN connections.

⌧ When the Network Mode has been changed to or away from *Transparent* mode, the device will reboot automatically.

⌧ If you change the address of the mGuard (e.g. by changing the Network Mode from *Transparent* to *Router*), the device will only be accessible at the new address.
When the change is done from the local interface, you will get a message telling you the new address before the change becomes active. When the change is done from the external interface you will not receive feedback from the mGuard.

⌧ If you set the Network Mode to *Router*, *PPPoE* or *PPTP* and then change the internal IP address and/or the local netmask, make very certain that you enter the correct values. Otherwise, the mGuard may no longer be accessible.

External IP Address

Address under which the mGuard is accessible for external network devices.

If the mGuard has been allocated an IP address dynamically, you will see here the IP address that is currently valid.

In *Transparent* mode, the mGuard assumes the address of the computer which is connected locally as its external IP.

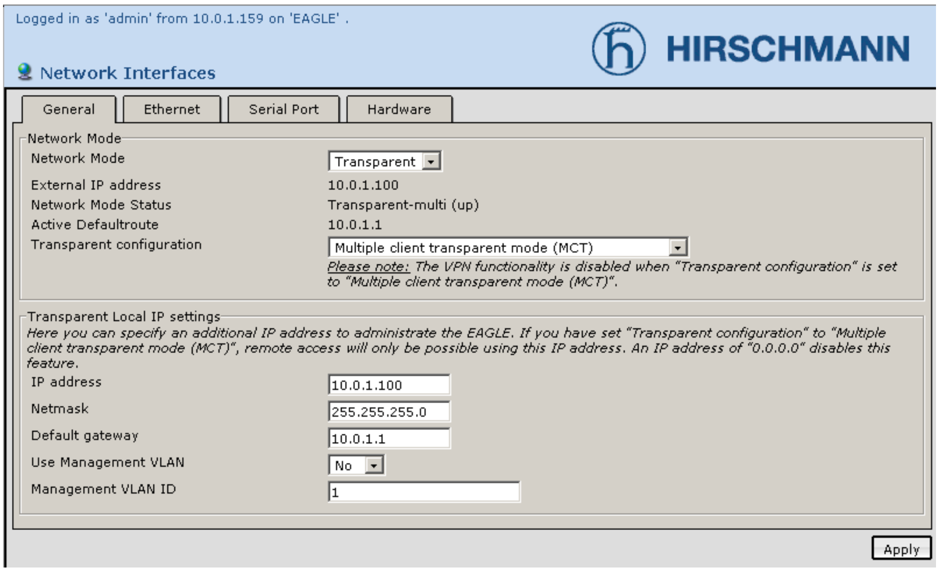
Network Mode Status

Displays the status of the selected network mode.

Active Default Route

Here the IP address is displayed via which the mGuard tries to reach networks that are unknown to it. The display will read "(none)" if the mGuard is running in *Transparent* mode, or if the IP address which has been defined in the configuration for the connected computer as the default gateway is not correct..

Network Mode → Transparent *(factory setting except mGuard delta)*



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Network Interfaces

General | Ethernet | Serial Port | Hardware

Network Mode

Network Mode	Transparent
External IP address	10.0.1.100
Network Mode Status	Transparent-multi (up)
Active Defaultroute	10.0.1.1
Transparent configuration	Multiple client transparent mode (MCT) *Please note: The VPN functionality is disabled when "Transparent configuration" is set to "Multiple client transparent mode (MCT)".*

Transparent Local IP settings

Here you can specify an additional IP address to administrate the EAGLE. If you have set "Transparent configuration" to "Multiple client transparent mode (MCT)", remote access will only be possible using this IP address. An IP address of "0.0.0.0" disables this feature.

IP address	10.0.1.100
Netmask	255.255.255.0
Default gateway	10.0.1.1
Use Management VLAN	No
Management VLAN ID	1

Network Mode

Transparent configuration

Single client transparent mode (SCT)autodetect

(Standard) The mGuard will analyse the network traffic and configure its network interface accordingly and will then function transparently.
For special cases, you can also preset these values, e.g. in the following case: The connected computer only accepts incoming connections so that it is not possible to configure the device automatically.

Single client transparent mode (SCT) static

If the mGuard cannot analyse the network traffic passing through, e.g. because the locally connected computer only receives data, the *Transparent configuration* must be set to **Static**.

Multiple client transparent mode (MCT)

Like **autodetect**, but it is possible to use multiple devices and IPs on the mGuard's internal interface (LAN).
For technical reasons VPN can't be used with this mode.

Transparent Local IP settings (Network Mode = Transparent)

An additional IP address can be specified here to administrate the mGuard. If

- *Transparent configuration* is set to the option **Multiple client transparent mode (MCT)** or
- the client doesn't answer ARP requests or
- there is no client at all,

then the remote administration via HTTPS, SNMP and SSH is only possible using the management IP address.

IP address

The additional IP address to contact the mGuard.

The IP address "0.0.0.0" disables the *Management IP Address*.

Netmask

The netmask for the IP address above.

Default Gateway

The default gateway of the network the mGuard is located in.

Use Management VLAN

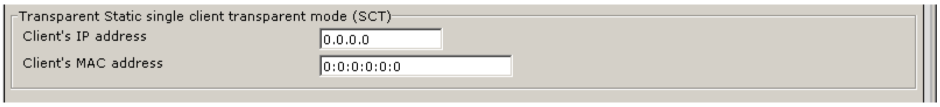
If this IP address is to be inside a VLAN, this option must be set to **Yes**. The mGuard supports in MCT and Router mode.

Management VLAN ID

A VLAN ID between 1 and 4095.

☞ An explanation of the term “VLAN” can be found under “VLAN” on page 153.

Transparent Static-Single-Client-Transparentmodus (SCT) (Transparent Configuration = static)



Transparent Static single client transparent mode (SCT)

Client's IP address	0.0.0.0
Client's MAC address	0:0:0:0:0:0

Client’s IP address

The IP address of the client.

Client’s MAC address

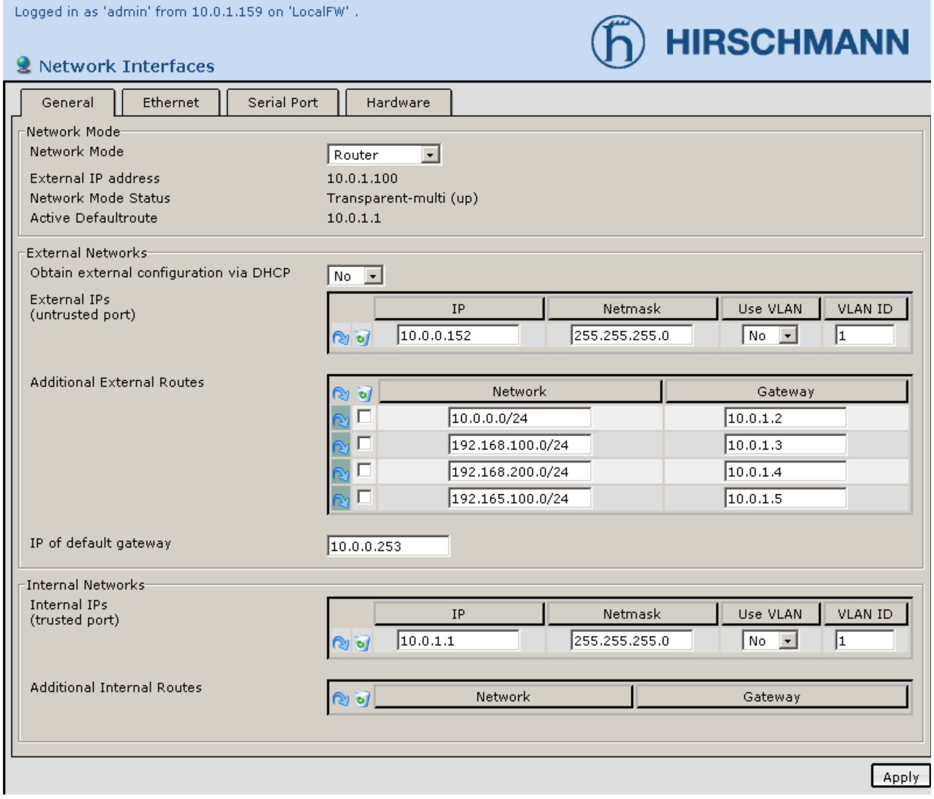
This is the physical address of the local computer’s network adapter to which the mGuard is connected.

⌦ **The MAC address can be determined in the following manner:**

On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter the following command:

```
ipconfig  /all
```

Network Mode → Router *(factory setting mGuard delta)*



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Network Interfaces

Network Mode

Network Mode	Router
External IP address	10.0.1.100
Network Mode Status	Transparent-multi (up)
Active Defaultroute	10.0.1.1

External Networks

Obtain external configuration via DHCP: No

External IPs (untrusted port)

IP	Netmask	Use VLAN	VLAN ID
10.0.0.152	255.255.255.0	No	1

Additional External Routes

Network	Gateway
10.0.0.0/24	10.0.1.2
192.168.100.0/24	10.0.1.3
192.168.200.0/24	10.0.1.4
192.165.100.0/24	10.0.1.5

IP of default gateway: 10.0.0.253

Internal Networks

Internal IPs (trusted port)

IP	Netmask	Use VLAN	VLAN ID
10.0.1.1	255.255.255.0	No	1

Additional Internal Routes

Network	Gateway

External Networks (Network Mode = Router)

These are the addresses under which the mGuard can be accessed by devices in the external networks (connected to the mGuard's Ethernet connector). If this unit is serving as a gateway to the Internet, the IP addresses will be assigned by the Internet Service Provider (ISP).

Obtain external configuration via DHCP: Yes / No

☞ If the mGuard obtains the configuration data via DHCP (Dynamic Host Configuration Protocol) from a DHCP server, enter **Yes**. In that case, all other entries made on this page will be ignored.

☞ If the mGuard does not obtain the configuration data via DHCP (Dynamic Host Configuration Protocol) from a DHCP server, enter **No** and make the following additional entries:

External IPs (untrusted port)

IP/Netmask

IP and netmask for the external interface (WAN).

Use VLAN

If this IP address is to be inside a VLAN, this option must be set to **Yes**.

VLAN ID

A VLAN ID between 1 and 4095.

☞ An explanation of the term “VLAN” can be found under “VLAN” on page 153.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 44.
(The first address in the list can’t be removed.)

Additional External Routes

In addition to the Default Route (see below), you can define additional, external routes.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 44.

IP of default Gateway

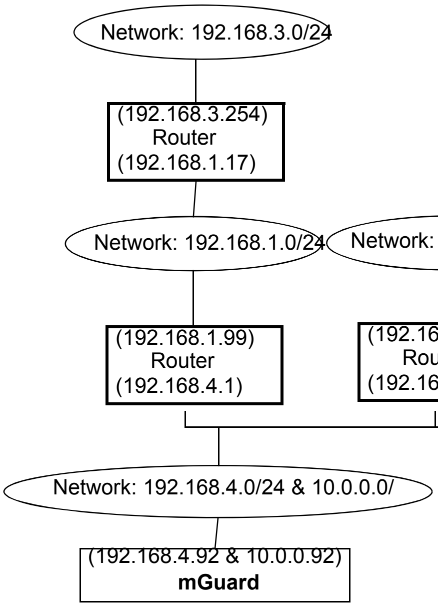
The IP address of a device in the local network (connected to the LAN port) or the IP address of a device in the external network (connected to the WAN port) can be specified here. If mGuard establishes the transition to the Internet, this IP address is specified by the Internet Service Provider (ISP). If mGuard is utilised within the LAN, the default gateway’s IP address will be specified by the network administrator. (See example sketch below).

⌧ If the local network is not known to the external router, e.g. in the case of configuration by DHCP, enter the address of your local network under Firewall → NAT, in other words 0.0.0.0/0 (see “Network Address Translation/IP Masquerading” on page 90)

Internal Networks

See “Network Mode → Router, PPPoE or PPTP” on page 60.

Example for the configuration of external networks:



For the szenario above the mGuard would have the following configuration:

external IPs:

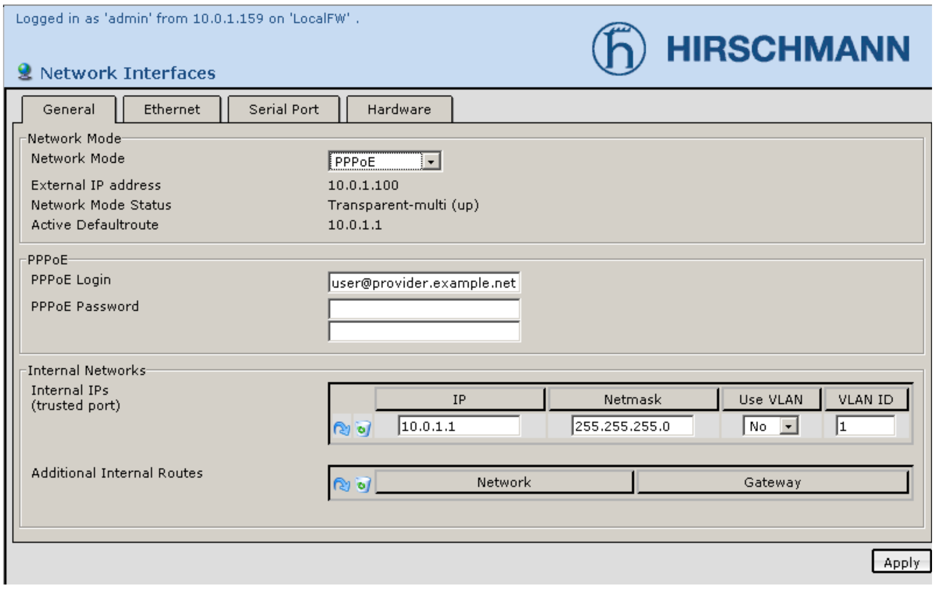
IP address	Networkmask
192.168.4.92	255.255.255.0
10.0.0.92	255.255.0.0

Additional external Routs:

Network	Gateway
192.168.2.0/24	192.168.4.2
192.168.1.0/24	192.168.4.1
192.168.3.0/24	192.168.4.1

IP of the Default Gateway:
192.168.4.254

Network Mode → PPPoE



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Network Interfaces

Network Mode

Network Mode	PPPoE
External IP address	10.0.1.100
Network Mode Status	Transparent-multi (up)
Active Defaultroute	10.0.1.1

PPPoE

PPPoE Login	user@provider.example.net
PPPoE Password	

Internal Networks

Internal IPs (trusted port)

IP	Netmask	Use VLAN	VLAN ID
10.0.1.1	255.255.255.0	No	1

Additional Internal Routes

Network	Gateway

PPPoE (Network Mode = PPPoE)

The Internet Service Provider (ISP) applies the user with a user name (Login) and a password for the access to the internet. When establishing a connection to the internet these will be requested.

PPPoE Login

In this field, enter the user name (Login), which is expected by your Internet Service Provider (ISP) when you setup a connection to the Internet.

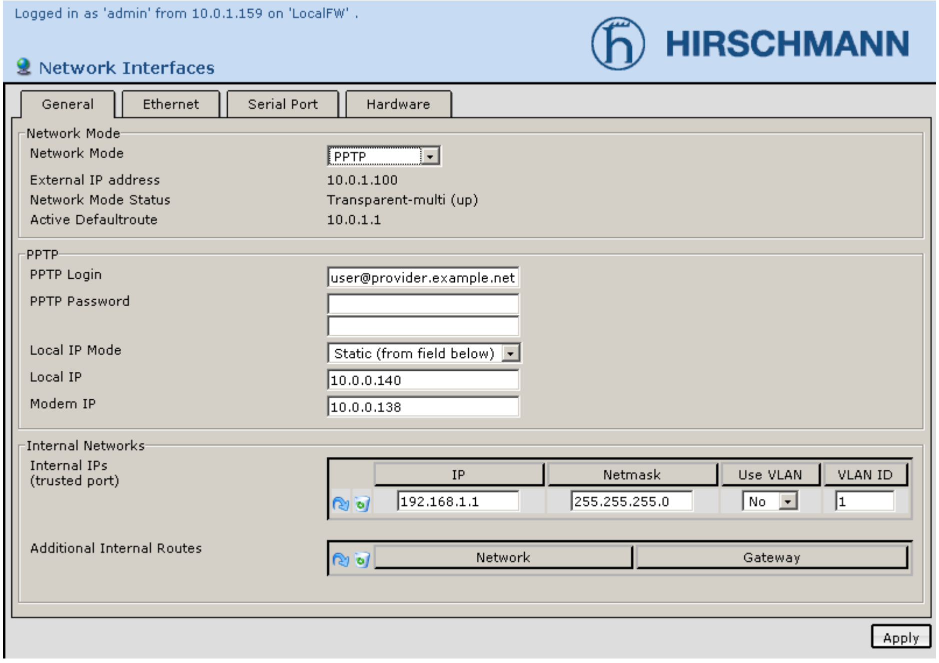
PPPoE Password

In this field, enter the password, which is expected by your Internet Service Provider when you setup a connection to the Internet.

Internal Networks

See “Network Mode → Router, PPPoE or PPTP” on page 60.

Network Mode → PPTP



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Network Interfaces

Network Mode

Network Mode	PPTP
External IP address	10.0.1.100
Network Mode Status	Transparent-multi (up)
Active Defaultroute	10.0.1.1

PPTP

PPTP Login	user@provider.example.net
PPTP Password	
Local IP Mode	Static (from field below)
Local IP	10.0.0.140
Modem IP	10.0.0.138

Internal Networks

Internal IPs (trusted port)

IP	Netmask	Use VLAN	VLAN ID
192.168.1.1	255.255.255.0	No	1

Additional Internal Routes

Network	Gateway

PPTP (Network Mode = PPTP)

PPTP Login

In this field, enter the user name (Login), which is expected by your Internet Service Provider when you setup a connection to the Internet.

PPTP Password

In this field, enter the password, which is expected by your Internet Service Provider when you setup a connection to the Internet.

Local IP Mode

Via DHCP

If the address data for the access to the PPTP server is supplied by the Internet Service Provider via DHCP, select **Via DHCP**.

In this case, you need not make an entry in the **Local IP** field.

Static (from field below)

If the address required to access the PPTP server is not supplied by the Internet Service Provider via DHCP, you must enter the IP address of the remote PPTP server and possibly that of the mGuard in the following two fields.

Local IP

The IP address under which the mGuard can be accessed by the PPTP server.

Modem IP

This is the address of the Internet Service Provider's PPTP server.

Internal Networks

See “Network Mode → Router, PPPoE or PPTP” on page 60.

Network Mode → Router, PPPoE or PPTP

Internal Networks (Network Mode is not Transparent)

Internal IPs

The Internal IP is the IP address, under which the mGuard can be accessed from the locally connected LAN.

In **Router** / **PPPoE** / **PPTP** mode, the default settings are:

IP address:	**192.168.1.1**
Local Netmask:	**255.255.255.0**

You can also specify other addresses, under which the mGuard can be accessed by devices on the locally connected network. This can be useful, for example, if the locally connected network is divided into subnetworks. In this case, multiple units on different subnetworks can access the mGuard under different addresses.

IP

IP-Adresse, under which the mGuard shall be accessible on the internal interface (LAN).

Netmask

A netmask for the internal interface (LAN).

Use VLAN

If this IP address is to be inside a VLAN, this option must be set to **Yes**. The mGuard supports in MCT and Router mode.

VLAN ID

A VLAN ID between 1 and 4095.

☞ An explanation of the term “VLAN” can be found under “VLAN” on page 153.

☞ The first entry in the list cannot be deleted.

Additional internal routes

If the locally connected network includes subnetworks, you can define additional routes.

Network

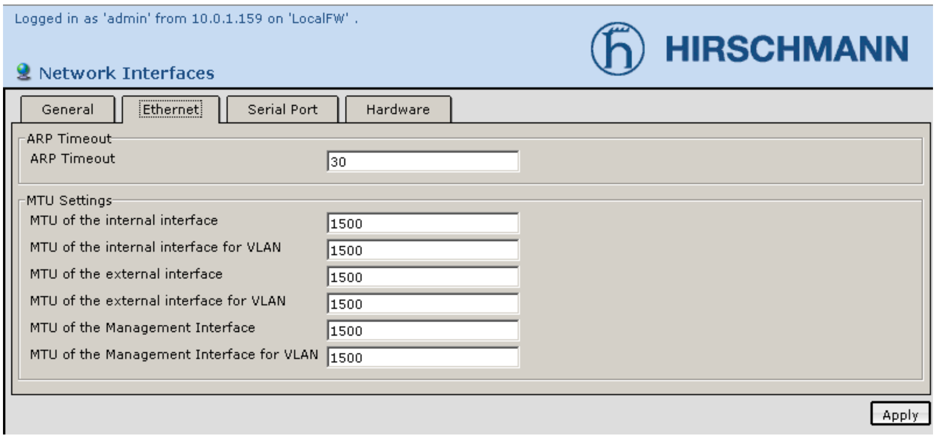
The network in CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

Gateway

The gateway used to reach this network.

☞ Siehe auch “Network Sketch” on page 141.

Ethernet



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Network Interfaces

ARP Timeout

ARP Timeout	30

MTU Settings

MTU of the internal interface	1500
MTU of the internal interface for VLAN	1500
MTU of the external interface	1500
MTU of the external interface for VLAN	1500
MTU of the Management Interface	1500
MTU of the Management Interface for VLAN	1500

ARP Timeout

ARP Timeout

Lifetime of entries in the ARP table.

MTU Settings

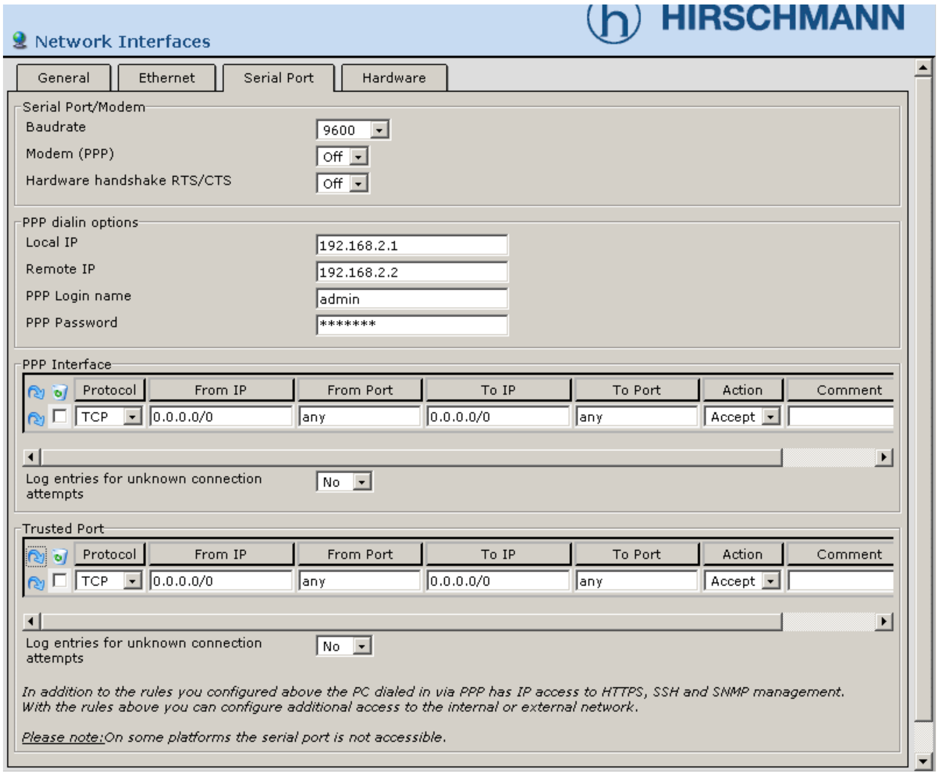
MTU of the ... interface

The Maximum Transfer Unit (MTU) defines the maximal frame size when sending from this interface and is usually 1500 for ethernet interfaces.

☒ VLAN interfaces

VLAN frames contain 4 bytes more than frames without VLAN which may cause problems with certain network equipment. By reducing the MTU to 1496 such problems can be avoided.

Serial Port *(only mGuard blade, delta and EAGLE mGuard)*



Serial Port/Modem

Baudrate	9600
Modem (PPP)	Off
Hardware handshake RTS/CTS	Off

PPP dialin options

Local IP	192.168.2.1
Remote IP	192.168.2.2
PPP Login name	admin
PPP Password	*******

PPP Interface

	Protocol	From IP	From Port	To IP	To Port	Action	Comment
□	TCP	0.0.0.0/0	any	0.0.0.0/0	any	Accept	

Log entries for unknown connection attempts: No

Trusted Port

	Protocol	From IP	From Port	To IP	To Port	Action	Comment
□	TCP	0.0.0.0/0	any	0.0.0.0/0	any	Accept	

Log entries for unknown connection attempts: No

In addition to the rules you configured above the PC dialed in via PPP has IP access to HTTPS, SSH and SNMP management. With the rules above you can configure additional access to the internal or external network.

Please note:On some platforms the serial port is not accessible.

Some mGuards, like the mGuard blade, delta or EAGLE, offer a serial V.24 interface with RJ45 socket which is accessible from the outside. The mGuard's configuration can also take place via this interface. The following possibilities are available:

- Connecting mGuard's serial interface to the serial interface of a PC. Establish the connection to the mGuard on a PC by using a terminal programme and carry out the configuration via SSH.
- Connect a modem, which is connected to the telephone (fixed-line or GSM) network, to the mGuard's serial interface. This enables a remote PC, also connected to the telephone network, by means of a modem to establish a PPP (Point-to-Point Protocol) dial-up connection to the mGuard. On a Windows PC, in order to be able to access mGuard's web configuration user interface using the PC's web browser via TCP/IP, you must set up a dial-up network connection to the mGuard.

Serial Port / Modem

Baudrate

The speed of the serial port.

MODEM (PPP)

When set to **Off** , the serial interface can be used with a terminal client. When set to **On**, the serial interface can be used with PPP.

Hardware handshake RTS/CTS

Use the RTS and CTS signals for the PPP connection.

PPP dialin options

Local IP

IP of the mGuard for the PPP connection.

Remote IP

IP of the remote peer for the PPP connection.

PPP Login name

Login to be send by the remote PPP peer.

PPP Password

Password to be send by the remote PPP peer.

Firewall Incoming (PPP-Interface)

Firewall rules for connection from the PPP to the internal ethernet interface (LAN).

You have the following options for the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

IP address

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets are passed through.

Reject means that the data packets are rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, Reject has the same effect as *Drop*.)

Drop means that the data packets are not passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

Comment

An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

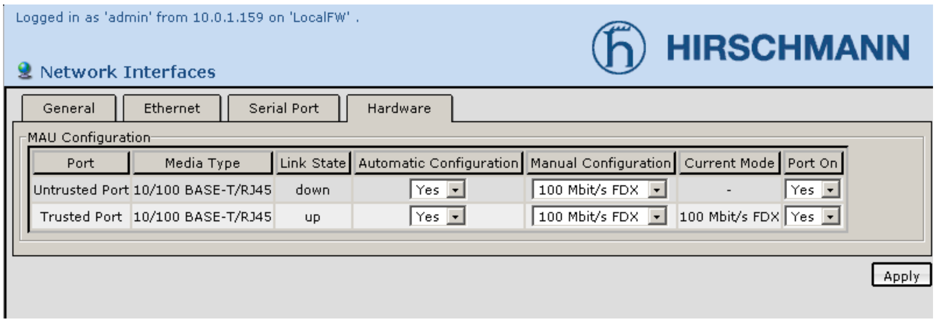
If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

Firewall Incoming (PPP-Interface)

Firewall rules for connection from the the internal ethernet interface (LAN) to PPP.

(All other settings conform to *Firewall Incoming (PPP-Interface)*.)

Hardware



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

MAU Configuration

Port	Media Type	Link State	Automatic Configuration	Manual Configuration	Current Mode	Port On
Untrusted Port	10/100 BASE-T/RJ45	down	Yes	100 Mbit/s FDX	-	Yes
Trusted Port	10/100 BASE-T/RJ45	up	Yes	100 Mbit/s FDX	100 Mbit/s FDX	Yes

Configuration and status display of the ethernet ports:

MAU Configuration

Port
Name of the interface the row refers to.

Media Type
Media type of the interface.

Link State
The state of the ethernet link which can be either **Up** or **Down**.

Automatic Configuration
When set to **Yes** the interface will be configured automatically. When set to **No**, the setting from the column **Manual Configuration** will be used.

⌧ Both ports of the mGuard are configured to be connected to a computer. If you connect the ports to a hub, please note that if *Automatic Configuration* is disabled, then the Auto-MDIX function will also be deactivated, i.e. the port of the mGuard has to be connected either to the uplink port of the hub or a cross-link cable has to be used.

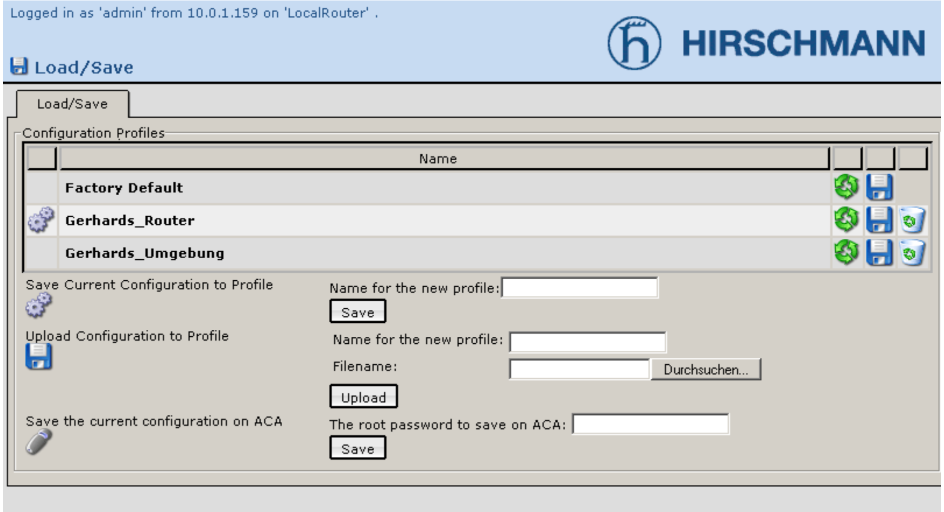
Manual Configuration
The configuration for the interface to be used when **Automatic Configuration** is set to **No**.

Current Mode
The current configuration of the interface.

Port on (only EAGLE and smart)
Enables/disables the port.

6.2.3 Basic Settings → Load/Save

Load/Save



Logged in as 'admin' from 10.0.1.159 on 'LocalRouter' .

Load/Save

Load/Save

Configuration Profiles

Name
Factory Default
Gerhards_Router
Gerhards_Umgebung

Save Current Configuration to Profile

Name for the new profile:

Save

Upload Configuration to Profile

Name for the new profile:

Filename: Durchsuchen...

Upload

Save the current configuration on ACA

The root password to save on ACA:

Save

You can save the configuration settings as a configuration profile under any name in the mGuard. You can create and save multiple configuration profiles. You can then select and activate the configuration profile appropriate at the time, if you use the mGuard in different operating environments.

Furthermore, you can also save configuration profiles as files on the configuration system. Naturally, these configuration files can then be read back into the mGuard and activated.

Furthermore, you can restore the mGuard to the factory settings at any time.

Also you can save configuration profiles on an external AutoConfiguration Adapter (ACA) which you can connect to the V.24 port - see “Profiles on the ACA (EAGLE mGuard only)” on page 66.

⌧Passwords and user names are not saved in the configuration profiles.

Configuration profiles

The top of the Configuration profile page has a list of configuration profiles that are stored in mGuard, for example, the Factory settings configuration profile. If any configuration profiles have been saved by the user (see below), they will be listed here.

Active configuration profile: The configuration profile that is currently in effect is shown with the *Aktive* symbol to the entry.

You can do the following with configuration profiles that are stored in mGuard:

- Activate them
- Save them to a file on the connected configuration computer
- Delete them
- Display them.

Displaying the configuration profile:

Click the name of the configuration profile in the list.

Applying the factory setting or a configuration profile setting that has been stored by the user

Click the **Restore** button located to the right of the name of the relevant configuration profile.

Result:

The corresponding configuration profile is activated.

⌧If the restoration involves a switch between the Transparent mode and another network mode, then mGuard is re-started.

Saving the configuration profile as a file to the configuration computer

1.Click the Download button to the right of the name of the respective configuration profile.

2.Specify the file name and folder in which the configuration profile is to be saved as a file in the displayed dialogue box. (You can give the file any name.)

Deleting a configuration profile:

Click the **Delete** button to the right of the name of the respective configuration profile.

⌧The **Factory settings** profile can’t be deleted.

Saving the current configuration as a configuration profile in mGuard

1. Enter the desired profile name in the name field behind “Save current configuration as profile.
2. Click the Save button.

Result:

The configuration profile is saved in mGuard, and the name of the profile is displayed in the list of profiles already saved in mGuard.

Uploading a configuration profile that has been saved to the configuration computer

Prerequisite: You have saved a configuration profile to the configuration computer as a file according to the procedure described above.

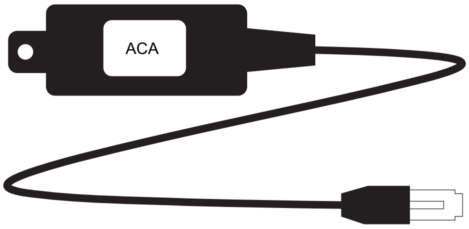
1. Enter the desired *new profile name* in the name field behind “Upload a configuration as profile“.
2. Click the **Browse**… button and select the respective file in the displayed dialogue box and open it..
3. Click the **Upload** button

Result:

The configuration profile is loaded into mGuard, and the name assigned in Step 1 will be displayed in the list of the profiles already stored in mGuard.

Profiles on the ACA (EAGLE mGuard only)

Configuration profiles also can be stored on an external *autoconfiguration adapter* (ACA) which is to be connected to the EAGLE mGuard’s V.24 (ACA11) or USB (ACA21) port. If both ACA´s are connected, the EAGLE mGuard prefers the ACA 21-USB.



Store a profile on the ACA

- When the password of the EAGLE mGuard, on which you will later import the profile, has a root password unequal “root” you must enter that password under **The root pasword to save on ACA**.
- Press the button **Save Current Configuration to ACA** to write the current configuration to the ACA.

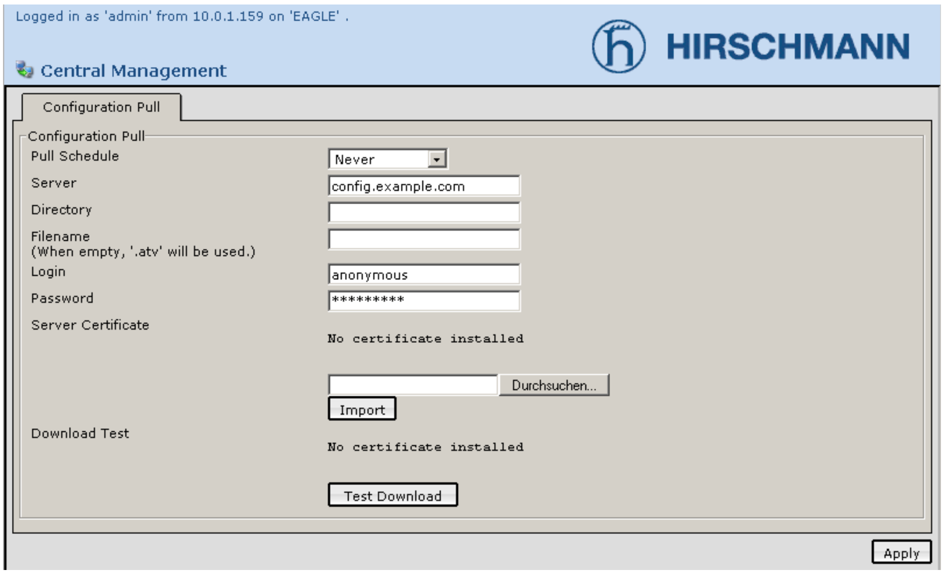
The LED STATUS and also the V.24 LED will blink until the store procedure is finished. The EAGLE mGuard saves the configuration into the file EAGLEmGuard.cfg on the ACA.

Restore profile from the ACA
Plug the ACA in mGuard’s V.24/USB socket. Start mGuard while the ACA is plugged in. The mGuard’s password has to be either ‘root’ or correspond to the password designated when saving the profile.
The STATUS LED and also the V.24 LED will flash until the loading process has ended.
Result:
The configuration profile with the name EAGLEmGuard.cfg is loaded from the ACA into the EAGLEmGuard and launched. It doesn’t appear in the list of configuration profiles stored in EAGLE mGuard.

⌦ The configuration on the ACA also includes the root, admin and user passwords, which will also be used when restoring a configuration from the ACA.

6.2.4 Basic Settings → Central Management

Configuration Pull



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Central Management

Configuration Pull

Configuration Pull

Pull Schedule: Never

Server: config.example.com

Directory:

Filename (When empty, '.atv' will be used.):

Login: anonymous

Password: *********

Server Certificate: No certificate installed

Download Test: No certificate installed

The mGuard can retrieve new configuration profiles from a HTTPS server in configurable time intervalls. When a new configuration differs from the current configuration, it will be activated automatically.

Configuration Pull

Pull Schedule

Intervall, at which new configurations will be searched on the server

Server

IP or Hostname of the server, which provides the configuration profiles.

Directory

The directory on the server in which the configuration is located.

Filename

The name of the file in the directory defined above. In case no filename is defined here, the name of the configuration file the mGuard's serial number with the suffix ".atv" is used.

Login

The login on the HTTPS server.

Password

The Password on the HTTPS server.

Server Certificate

The certificate, which authenticates the HTTPS server from which the configuration is fetched. It is used to prevent unauthorized configurations from being installed on the mGuard.

☞ In case the configuration profiles do contain the machine certificate or PSKs for VPN connections the password should consist of at least 30 random upper and lower case letters and numbers, in order to prevent unallowed access to the keys.
The HTTPS server should further only grant access to a single configuration profile per login and password. Otherwise users of other or even compromised mGuards may gain access to other configurations.

☞ The IP address or the hostname specified under *Server* must be the same as the certificates Common Name (CN) entry.

☞ Self signed certificates should not use the "key-usage" extension.

☞ In case the server certificate is self signed, that server certificate must be imported here. In case the certificate was signed by a certification authority (CA), the CA's certificate must be imported here.

To install the certificate perform the following steps:

1. Click on **Browse...** so select the certificate file.
2. Click on **Import**.

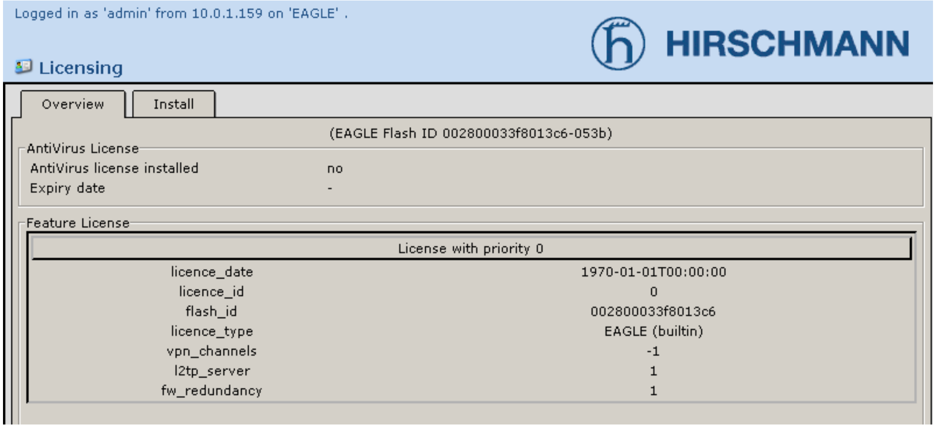
Download Test

By clicking on **Test Download** you can test – without actually saving the modified parameters or activating the profile – if the parameters are correct. The result of the test will be displayed in the right column.

⌧ You should make sure that the profile on the server doesn't contain unwanted variables beginning with "GAI_PULL_" which overwrite the pull configuration made here.

6.2.5 Basic Settings → Licensing

Overview



(EAGLE Flash ID 002800033f8013c6-053b)

AntiVirus License

AntiVirus license installed	no
Expiry date	-

Feature License

License with priority 0	
licence_date	1970-01-01T00:00:00
licence_id	0
flash_id	002800033f8013c6
licence_type	EAGLE (builtin)
vpn_channels	-1
l2tp_server	1
fw_redundancy	1

AntiVirus License

Anti-Virus license installed

Here you can examine the validity of the installed AVP license.

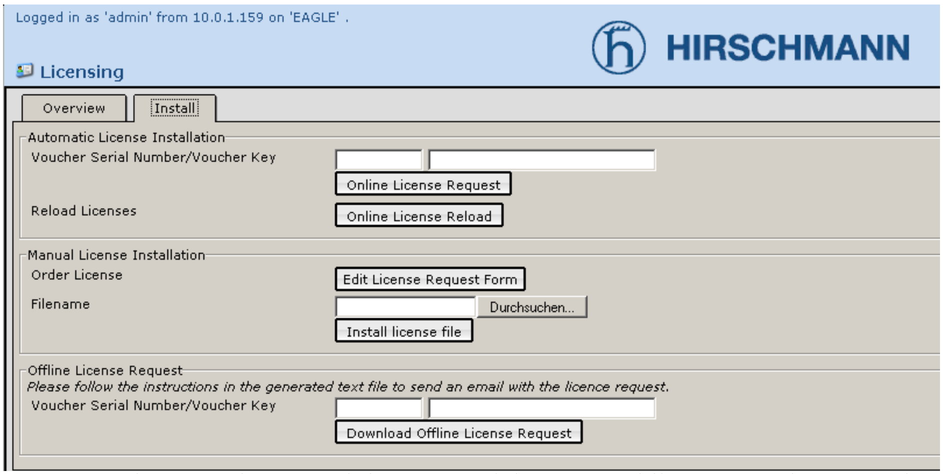
Expiry date

Shows the expiry date of your anti-virus license.

Feature License

Shows which functions are included with the mGuard license you have purchased, e.g. the number of possible VPN tunnels.

Install


Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .
HIRSCHMANN
Licensing
Overview
Install
Automatic License Installation
Voucher Serial Number/Voucher Key
Online License Request
Reload Licenses
Online License Reload
Manual License Installation
Order License
Edit License Request Form
Filename
Durchsuchen...
Install license file
Offline License Request
Voucher Serial Number/Voucher Key
Download Offline License Request

Please follow the instructions in the generated text file to send an email with the licence request.

You can subsequently expand the range of the mGuard license you have purchased with further functions. In this window, you will find a license or voucher key and a license or voucher serial number. With these, you can

1. request the necessary feature license file, before
2. installing the license file which you will then receive.

Automatic license installation

Voucher Serial Number/Voucher Key

Enter here the serial number that is printed on the voucher, as well as the accompanying license key and then click

Online License Request.

Result:

mGuard now establishes a connection via the Internet and installs the respective license on the mGuard if the voucher is valid.

Restoring licenses

Use this function if the license installed in mGuard has disappeared for some reason, such as flashing the firmware. To do so, click the **Online license restoration** button. The license(s) that had been issued for this mGuard previously will be retrieved from the server and installed.

Manual license installation

After clicking the **License Request Form** button, an online form will be provided which can be used to order the desired license. On the request form, enter the following information:

Voucher Serial Number: the serial number that is printed on your voucher

Voucher Key: the license key on your voucher

Flash Id: is automatically filled in

Email Address: the email address to which the license file will be sent

After you have completed the form, the license file will be sent to the email address indicated. Under *Filename* you can apply the license file.

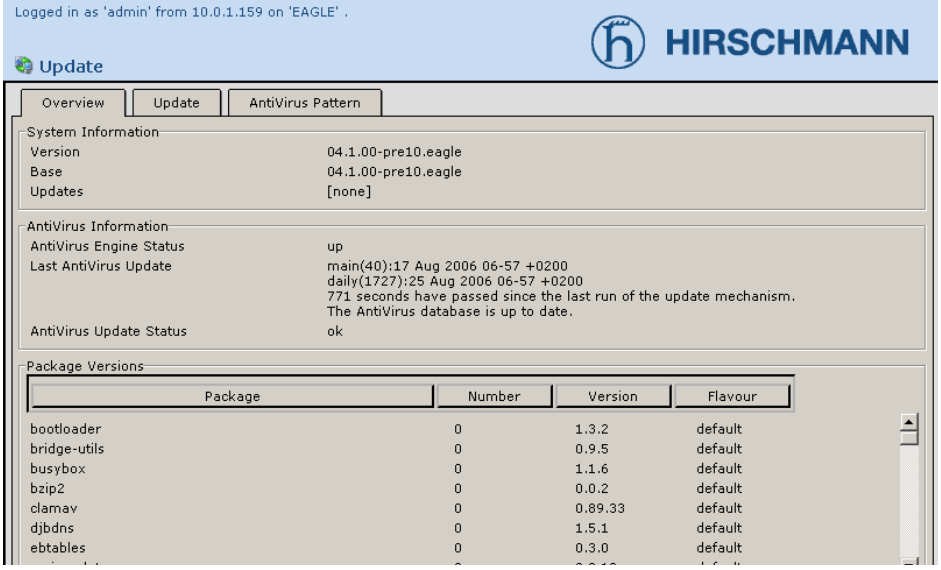
Install License

Once the license has been purchased, the license file will be sent to you as an email attachment. In order to apply the license, first save the license file as a separate file on your computer and continue as follows:

– Click the **Browse** button, select the file and open it so that the path or the file name is displayed in the *File Name* field.
– Then click the **Install License File** button.

6.2.6 Basic Settings → Update

Overview



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Update

System Information

Version	04.1.00-pre10.eagle
Base	04.1.00-pre10.eagle
Updates	[none]

AntiVirus Information

AntiVirus Engine Status	up
Last AntiVirus Update	main(40):17 Aug 2006 06-57 +0200 daily(1727):25 Aug 2006 06-57 +0200 771 seconds have passed since the last run of the update mechanism. The AntiVirus database is up to date.
AntiVirus Update Status	ok

Package Versions

Package	Number	Version	Flavour
bootloader	0	1.3.2	default
bridge-utils	0	0.9.5	default
busybox	0	1.1.6	default
bzip2	0	0.0.2	default
clamav	0	0.89.33	default
djbdns	0	1.5.1	default
ebtables	0	0.3.0	default

You can examine the successful clearing of the of the virus filter feature.

For the information about the expiration date of your anti-virus license please see “Basic Settings → Licensing” on page 69

System Information

Version

The current software version of the mGuard

Base

The software version that was originally used to flash this mGuard.

Updates

List of updates that have been installed on the base.

AntiVirus Information

Anti-Virus Engine Status

Displays the state of the scan-engine. If you have activated the anti-virus protection for at least one protocol, the status will be displayed as “up”.

Last Anti-Virus Update

Diplays the current release date of the anti-virus database as well as the time which is passed through since the last update in seconds and if the AntiVirus database has the current state.

The database is made up of the files main.cvd and daily.cvd, whereas the latter is updated frequently.

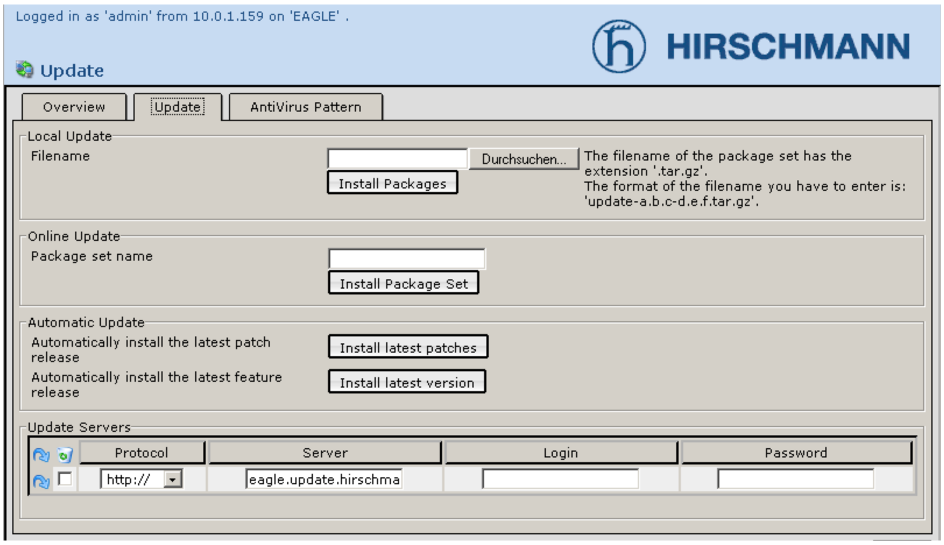
Anti-Virus Update Status

Shows if the anti-virus update is activated or currently downloading

Package Versions

Lists the individual software modules of the mGuard. Could be used for support purposes, as applicable.

Update



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Update

Local Update

Filename: The filename of the package set has the extension '.tar.gz'. The format of the filename you have to enter is: 'update-a.b.c-d.e.f.tar.gz'.

Online Update

Package set name

Automatic Update

Automatically install the latest patch release

Automatically install the latest feature release

Update Servers

	Protocol	Server	Login	Password
□	http://	eagle.update.hirschma		

There are two possibilities for conducting a software update:

– You have the updated package set file on your computer (the file name ends with ".tar.gz") and you conduct a local update.

OR

– You can download the package set file via the Internet from the update server and then install the packet.

☒ Depending on the size of the update, this may take several minutes.

☒ If a reboot is necessary after a system update, a message to this effect will be displayed.

☒ Do not interrupt the power supply during the update procedure! Otherwise the device could be damaged and may be left inoperable, and will require your device to be send to the manufacturer.

Local Update

Filename

To install the packages proceed as follows:

1. Click on **Browse...** , select and open the file so that that its path or file name is shown in the field Filename.
   The format of the filename is: update-a.b.c-d.e.f.tar.gz.
2. Click on **Install Packages** to transfer them to the device.

Online Update

To perform an online update proceed as follows:

1. Be sure that at least one valid entry exists under **Update Server**. You should have received the necessary details from your licensor.
2. Enter the update’s name in the entry field, e.g. “update-4.0.x-4.1.0”.
3. Click on **Install Package Set** to transfer them to the device.
   Depending on the size of the update, this may take several minutes.

If a reboot is necessary after a system update, a message to this effect will be displayed.

Automatic Update

This is a variation of the online update in which the mGuard independently determines the required package set name.

Automatically install the latest patch release

Patch releases regulate errors in previous versions and have a version number which only changes in the third digit position:

e.g. 4.0.1 is a patch release for version 4.0.0.

Automatically install the latest feature release

Feature releases supplement the mGuard with new attributes or contain modifications to the behavior of the mGuard. Their version number only change in the first and second digit position.

e.g. 4.1.0. is a feature release for the versions 3.1.0. and 4.0.1.

Update Servers

Here you can specify the servers from which the mGuard shall retrieve its updates.

⌧The list of the servers is processed top-down until an available server is found.

Protocol

The update files can be downloaded using either HTTP or HTTPS.

Server

In this field, enter the FQDN or IP address of the server from which the update files shall be downloaded, eg. “123.456.789.21” or “update.example.com”.

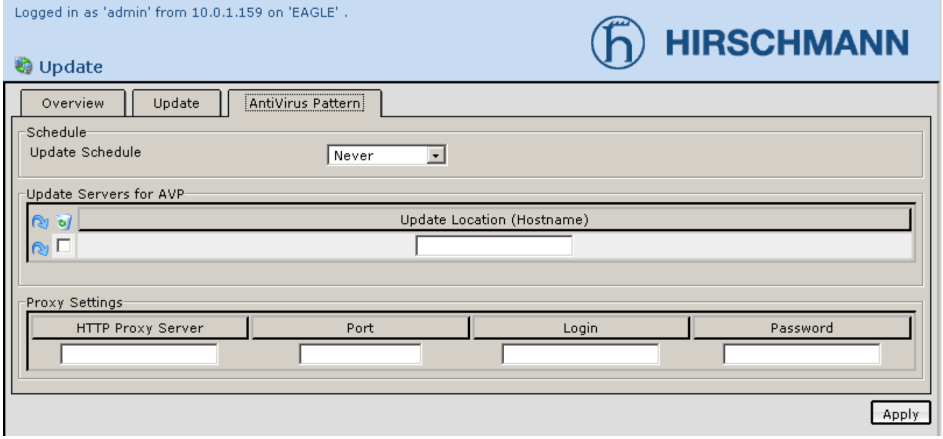
Login

In this field, enter the user name to be used for connecting to the server.

Password

In this field, enter the password to be used when logging in.

AntiVirus Pattern



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Update Schedule: Never

The virus signature files can be updated from a selected update server at intervals defined by the user. The update is performed without interrupting the operation of the anti-virus filter. The mGuard is delivered without any virus signatures installed. Therefore, after the anti-virus protection has been activated with the corresponding license, you should also set the update schedule. The course of the updates can be examined in the Event Logs by selection of anti-virus Update.

Schedule

Update Schedule

This parameter is used to set how often the signature files are updated. The size of the signature file is currently about 5 MByte. The system will only download the updated files from the update server.

Update Servers for AVP

You can select the server from which the updated signature files should be downloaded. A default server has already been entered. If necessary, you can enter your own servers.

⌧The list of servers will be processed from the top down until an available server is found.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 44.

Proxy Settings

When the mGuard is located behind a firewall which restricts HTTP or FTP access to use a proxy server, the following rows can be used to specify the required proxy settings.

☞ For the proxy server to be used the fields **HTTP/FTP Proxy Server** *and* **Port** must be set.

☞ To authenticate with the proxy server the fields **Login** *and* **Password** must be set.

HTTP/FTP Proxy Server

The proxy servers IP or hostname.

Port

The port belonging to the IP or hostname of the proxy server.

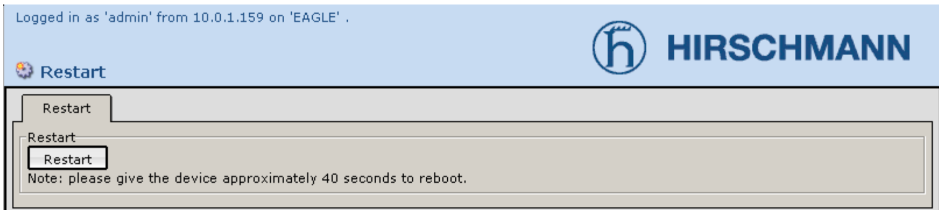
Login

The login in case the proxy server requires authentication.

Password

The password belonging to the login.

6.2.7 Basic Settings → Restart



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Note: please give the device approximately 40 seconds to reboot.

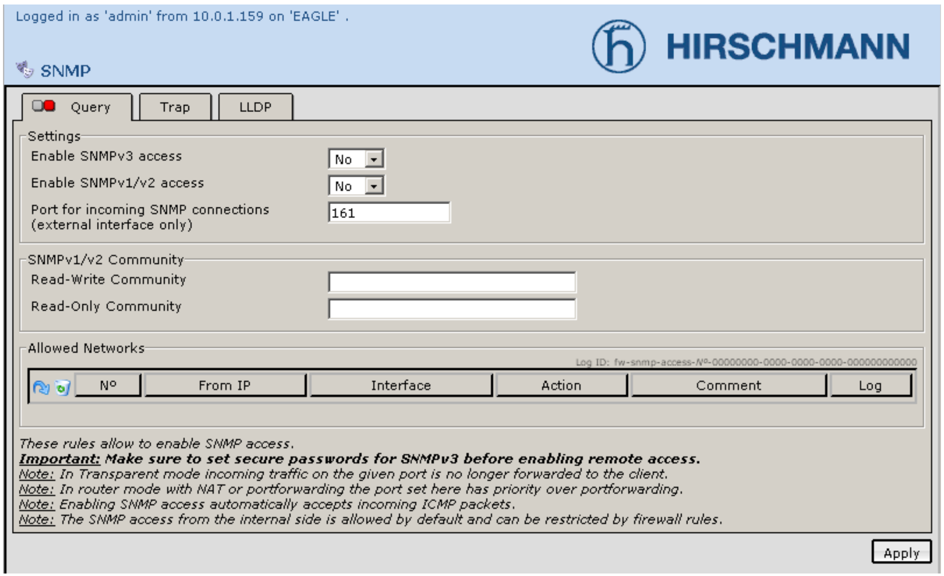
A new start (= reboot) is necessary in the event that a fault occurs. It may also be necessary after a software update.

(You can also reboot the device by switching it off and back on again.)

6.3 Menu Security

6.3.1 Security → SNMP

Query



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

SNMP

Query | Trap | LLDP

Settings

Enable SNMPv3 access: No

Enable SNMPv1/v2 access: No

Port for incoming SNMP connections (external interface only): 161

SNMPv1/v2 Community

Read-Write Community:

Read-Only Community:

Allowed Networks

Log ID: fw-snmp-access-Nº-00000000-0000-0000-0000-000000000000

Nº	From IP	Interface	Action	Comment	Log

These rules allow to enable SNMP access.

***Important:* Make sure to set secure passwords for SNMPv3 before enabling remote access.**

Note: In Transparent mode incoming traffic on the given port is no longer forwarded to the client.

Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.

Note: Enabling SNMP access automatically accepts incoming ICMP packets.

Note: The SNMP access from the internal side is allowed by default and can be restricted by firewall rules.

SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the status and operation of devices.

SNMP is available in several releases: SNMPv1/SNMPv2 and SNMPv3.

The older versions SNMPv1/SNMPv2 do not use encryption and are not considered to be secure. We therefore recommend that you do not use SNMPv1/SNMPv2.

As far as security is concerned, SNMPv3 is considerably better, but not all management consoles support it.

The Hirschmann Network Management HiVision communicates via SNMPv1 with the devices.

The Network Management System Industrial HiVision can communicate via SNMPv1/SNMPv2 and SNMPv3 with the devices. Recommendable is using SNMPv3.

⌦ It can take more than one second to process SNMP- “get” or “walk” requests. However the factory settings for the time-out of many Network Management Applications is set to one second. In case you experience time-out problems, please set the time-out of your Management Application to values between 3 and 5 seconds.

Settings

Enable SNMPv3 access: Yes / No

If you wish to allow monitoring of the mGuard via SNMPv3, set this switch to **Yes**.

The access via SNMPv3 requires an authentication with a login and a password. The factory settings for these entries are:

Login: admin
Password: private (EAGLE mGuard)

MD5 is supported for the authentication; DES is supported for encryption.

The login parameters for SNMPv3 can be changed only by using SNMPv3.

Example for changing the SNMPv3 password via Industrial HiVision.

1. Click on the mGuard and in the menu bar of Industrial HiVision select "Tools:SNMP Browser".
2. In the menu bar of the SNMP Browser select "Edit:SNMP Configuration".

3. In the "Protocol Version" frame of the "SNMP Configuration" dialog click on "V3 (USM)".
4. In the filecard "V3 (USM)" of the "SNMP Configuration" dialog enter the username (state of delivery: "admin").
5. In the "Authentication" frame of the filecard "V3 (USM)" of the "SNMP Configuration" dialog click on "MD5" and entert he password (state of delivery: "private").
6. In the "SNMP Configuration" dialog click on **Close** to close the window.
7. in the menu bar of the SNMP Browser select "Edit:SNMPv3 Usermanagement".
   Click on **Reload** to see existing enties.
8. Click on **Change Password**.
9. In the line "Old authentication Password" entert he old SNMPv3 password (stateo f delivery: "private").
10. In the line "New Authentication Password" entert he new SNMPv3 password.
11. Click on **Change** to apply the changes and close the window.

Enable SNMPv1/v2 access: Yes / No

If you wish to allow monitoring of the mGuard via SNMPv1/v2, set this switch to **Yes**.

Port for incoming SNMP connections (external interface only)

Standard: 161

SNMPv1/v2 Community

Read-Write Community

Read-Only Community

Enter the required login data in these two fields.

Allowed Networks

Lists the firewall rules that have been set. These apply for the incoming data packets of an SNMP remote access.

From IP

Enter the address(es) of the system(s) that is/are allowed access for the purpose of SNMP monitoring in this field.

You have the following options for the entries:

- An IP address.
- To enter an address space, use the CIDR notation – see "CIDR (Classless InterDomain Routing)" on page 140.
- 0.0.0.0/0 means all addresses.

Interface

Indicates whether the rule applies to the external interface (= ungesicherter port) or the internal interface (= gesicherter port).

Action

Possible settings:

- Accept
- Reject
- Drop

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, *Reject* has the same effect as *Drop*.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

☞ In Transparent mode, *Reject* is not supported.

Comment

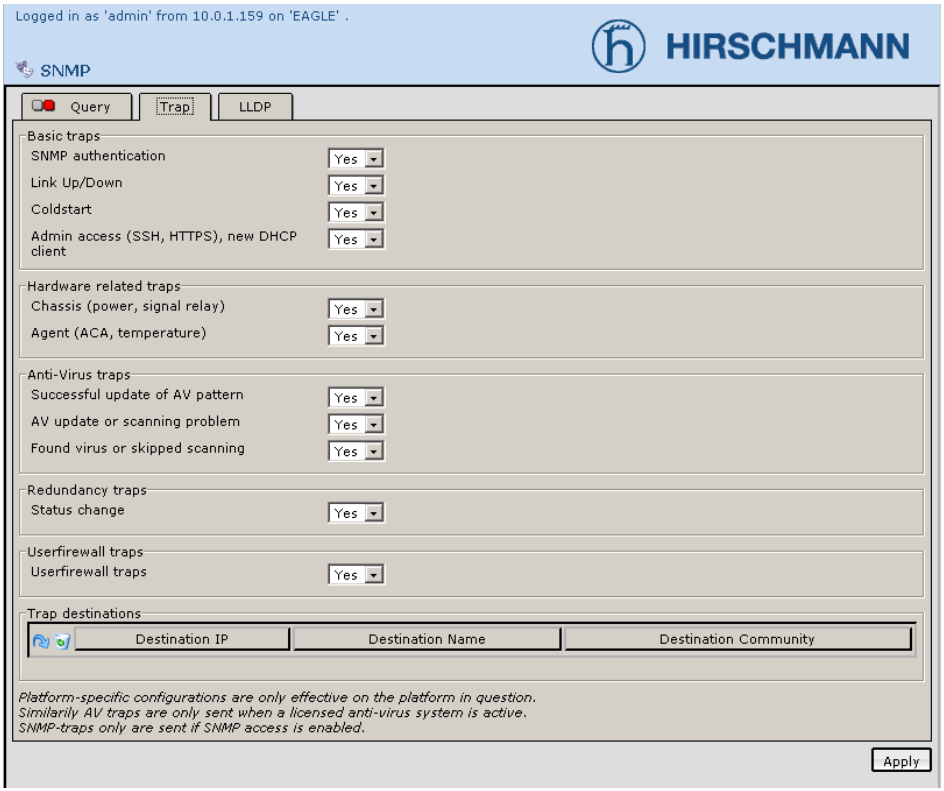
An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

- should be logged by setting - *Log* to **Yes**
- or should not be logged by setting - *Log* to **No** (factory setting).

Trap



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

HIRSCHMANN

SNMP

Query | Trap | LLDP

Basic traps

SNMP authentication	Yes
Link Up/Down	Yes
Coldstart	Yes
Admin access (SSH, HTTPS), new DHCP client	Yes

Hardware related traps

Chassis (power, signal relay)	Yes
Agent (ACA, temperature)	Yes

Anti-Virus traps

Successful update of AV pattern	Yes
AV update or scanning problem	Yes
Found virus or skipped scanning	Yes

Redundancy traps

Status change	Yes

Userfirewall traps

Userfirewall traps	Yes

Trap destinations

Destination IP	Destination Name	Destination Community

Platform-specific configurations are only effective on the platform in question.
Similarily AV traps are only sent when a licensed anti-virus system is active.
SNMP-traps only are sent if SNMP access is enabled.

Apply

On certain events the mGuard can send SNMP traps. These traps are compatible with SNMPv1. For each settings the traps being send are explained in the MIB file on the product CD-ROM or under www.hirschmann-ac.com.

SNMP Trap Destinations

Traps can be send to one or more targets.

Destination IP

IP, to which the trap shall be send.

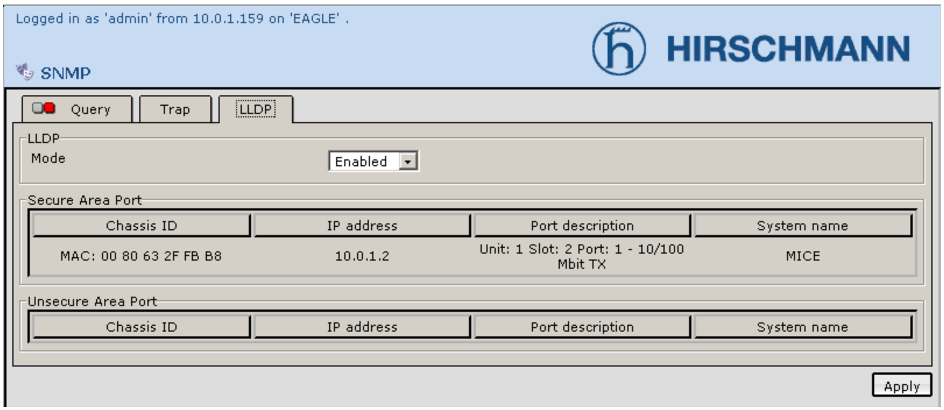
Destination Name

An optional descriptive name for the destination, which has no influence on the generated traps.

Destination Community

Name of the traps SNMP community.

LLDP



LLDP

Mode: Enabled

Secure Area Port

Chassis ID	IP address	Port description	System name
MAC: 00 80 63 2F FB B8	10.0.1.2	Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX	MICE

Unsecure Area Port

Chassis ID	IP address	Port description	System name

LLDP (Link Layer Discovery Protocol, IEEE 802.1AB) supports the automatic detection of the (ethernet) network topology.

LLDP capable devices periodically send ethernet multicasts (layer 2) with network information about themselves which will be collected by other LLDP capable devices and made available via SNMP.

⌧ The Hirschmann Network Mangement System Industrial HiVision uses LLDP for topology discovery. Enable LLDP on the EAGLE mGuard if you use Industrial HiVision.

LLDP

Mode

Enabling and disabling of the LLDP service.

Internal/LAN interface and External/WAN interface

Chassis ID

An entity which identifies a remote device uniquely; typically one of its MAC addresses.

IP address

The IP address to manage the remote device via SNMP.

Port description

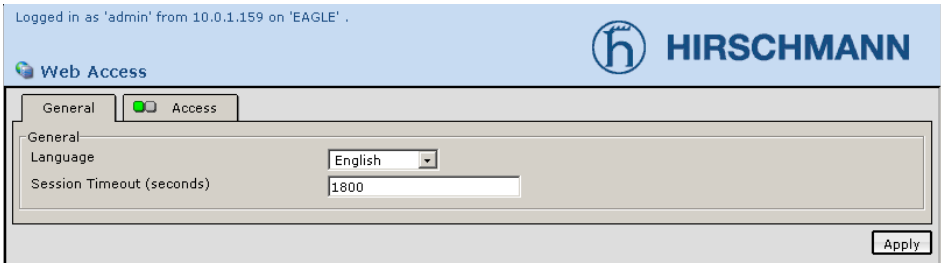
A textual description of the remote device's interface.

System name

Hostname of the remote device.

6.3.2 Security → Web Access

General



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Web Access

General | Access

General

Language	English
Session Timeout (seconds)	1800

General

Language

If **(Automatic)** is selected from the list of languages, the device will use the language setting of the system‘s browser.

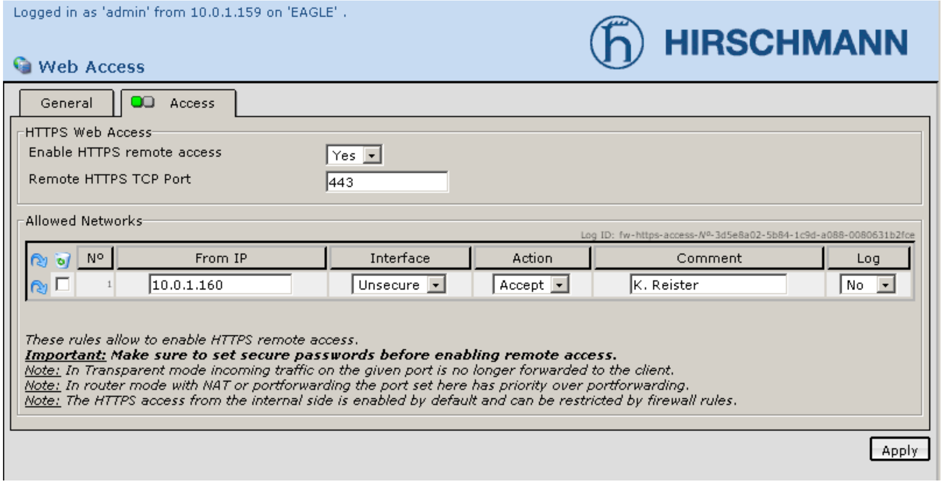
Session Timeout (seconds)

Specifies the time interval of inactivity (in seconds) after which the user will be logged out automatically. Possible values are between 15 and 86400 (= 24 hours) seconds.

Scope of the ’Apply’ button

If set to **per Page**, configuration changes need to be applied per page for being stored. Otherwise (**per Session)** the configuration may be changed on several pages before being applied

Access



Logged in as 'admin' from 10.0.1.159 on 'EAGLE' .

Web Access

General | Access

HTTPS Web Access

Enable HTTPS remote access	Yes
Remote HTTPS TCP Port	443

Allowed Networks

Log ID: fw-https-access-Nº-3d5e8a02-5b84-1c9d-a088-0080631b2fce

	Nº	From IP	Interface	Action	Comment	Log
□	1	10.0.1.160	Unsecure	Accept	K. Reister	No

These rules allow to enable HTTPS remote access.
***Important:* Make sure to set secure passwords before enabling remote access.**
Note: In Transparent mode incoming traffic on the given port is no longer forwarded to the client.
Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.
Note: The HTTPS access from the internal side is enabled by default and can be restricted by firewall rules.

HTTPS Web Access

When HTTPS Remote Access is enabled, the mGuard can be configured – using its Web-based Administrator interface – from a remote system. In other words, a browser running on the remote system will be used to configure the local mGuard.
This option is disabled by default.

IMPORTANT:If you enable remote access, make certain that you have secure root and administrator passwords.

To enable HTTPS remote access, proceed as follows:

Enable HTTPS remote access: Yes / No

If you want to enable a HTTPS connection, set this switch to **Yes**.

☞ In this case, make certain that the firewall rules on this page permit the mGuard be accessed from a remote site.

Port for incoming HTTPS connections (remote administration only)

Standard: 443

You can select a different port.

If a different port has been selected, you must append the port number (set here) to the IP address of the device in the address provided by the remote site, which will have remote access.

Example:

If this mGuard can be found in the Internet at the address 123.456.789.21 and the Port Number 443 has been set as the port for remote access, you need not enter this port number after the address in the Web browser's address field on the remote system.

If a different Port Number is used, this must be appended to the IP address, e. g as follows.: https://123.456.789.21:442/

Allowed Networks

Lists the firewall rules that have been set. These apply for the incoming data packets of an HTTPS remote access.

From IP

Enter the address(es) of the system(s) that is/are allowed remote access in this field.

You have the following options for the entries:

- IP address: **0.0.0.0/0** means all addresses. To enter an address space, use the CIDR notation – see "CIDR (Classless InterDomain Routing)" on page 140.

Interface

Trusted OR **Untrusted**

Defines for which interface the rule applies, the trusted port or the untrusted port.

State on delivery: the untrusted port discards all, the trusted port accepts all.

Action

Possible settings:

- Accept
- Reject
- Drop

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, *Reject* has the same effect as *Drop* see below.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

☞ In Transparent mode, *Reject* is not supported.

Comment

An informational comment for this rule.

Log

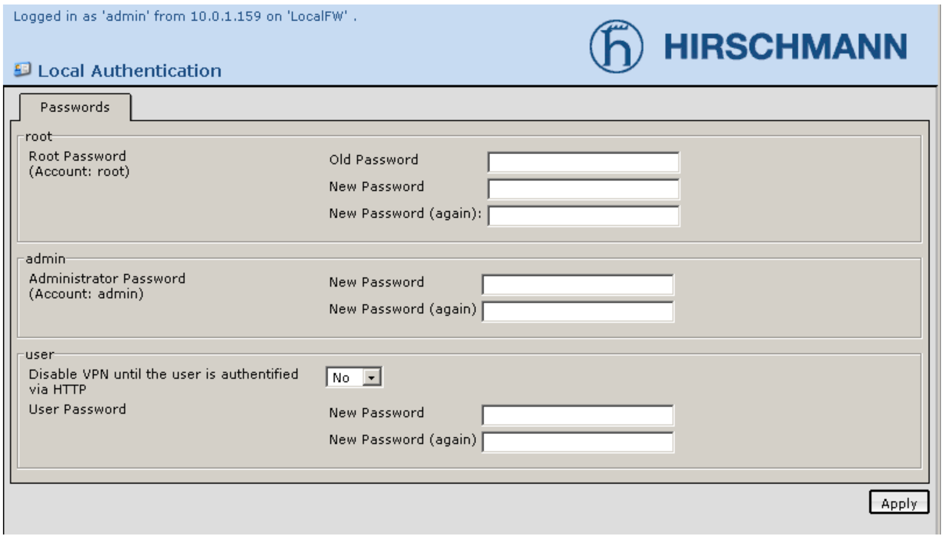
You can specify – for each individual firewall rule – whether the use of the rule

- should be logged by setting - *Log* to **Yes**
- or should not be logged by setting - *Log* to **No** (factory setting).

6.3.3 Security → Local Authentication

The term Local Authentication refers to users who have the right, depending on their access permission level, to configure mGuard (‘root’ and ‘administrator’ access permission) or to use it (‘user’ access permission).

Passwords



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Local Authentication

Passwords

root

Root Password (Account: root)

Old Password

New Password

New Password (again):

admin

Administrator Password (Account: admin)

New Password

New Password (again)

user

Disable VPN until the user is authentified via HTTP: No

User Password

New Password

New Password (again)

The mGuard supports 3 levels of user authorization. To login at a specific level of authorization, the user must enter the corresponding password for the level.

Authorization level	
Root	This level (password) grants full rights to all parameters of the mGuard. Note: This is the only authorization level that allows you to setup a SSH connection to the device and to then change all of the parameters so that nothing will work any more. If this happens, all you can do is “flash” the firmware to restore it to the factory settings (see “Flashing the firmware” on page 143). Default root password: **root**
Administrator	If you login at this level (password), you will be granted all the rights required for the configuration options that are accessible via the Web-based Administrator interface. Default user name: **admin** Default password: **private** (EAGLE mGuard) The user name **admin** cannot be changed.
User	If a user password has been defined and activated, the user must – after every restart of the mGuard – enter this password to enable a VPN connection when he or she first attempts to access any HTTP URL. If you wish to use this option, enter the desired user password once in each of the corresponding entry fields. (Note: As long as a required user login hasn't taken place, it might happen that some other services on the mGuard can't be started or can't be easily re-configured.)

root

Root Password

Factory (default) setting: **root**

If you wish to change the root password, enter the current password in the *Old Password* field and then the desired new password in the two corresponding fields below.

admin

Administrator Password (Account: admin)

Factory (default) setting: **private** (fixed user name: admin)

user

Disable the VPN until the user is authenticated via HTTP:

Yes / No

The factory→ default setting for this switch is No.

In the case of Yes, a VPN connection can only be used after the user establishes any HTTP (e.g., www.google.com) connection, because this is needed in order to log in (= enter the user password). Also, a user password needs to have been specified.

User Password

There is no factory setting for the user password. To set one, enter the desired password twice - once in each of the two fields.

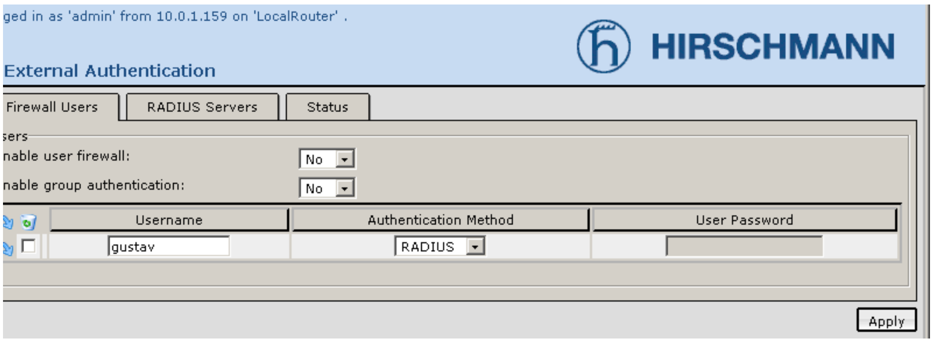
6.3.4 Security → External Authentication

The Firewall users group members overlap with the local users members ('user' access permission level) or may even be identical. The only difference is as follows: Individuals that are registered (through allocation of user name / password) can have individually tailored firewall rules assigned to them.

Example:

> To eliminate private surfing on the Internet, every outgoing connection is blocked (VPN is not affected) by means of outgoing filter rules via Network Security → Packet filters. Under Network Security → User firewall, certain user firewalls can be assigned different firewall rules definitions, for example, permitting any outgoing connection. This user firewall rule goes into effect as soon as any respective firewall user to whom this firewall rule applies has logged in, (see "Network Security → User Firewall" on page 95).

Remote Users



ged in as 'admin' from 10.0.1.159 on 'LocalRouter' .

External Authentication

sers

nable user firewall: No

nable group authentication: No

Username	Authentication Method	User Password
gustav	RADIUS	

User

List of external users: their user names and authentication methods

Activate User Firewall: Yes / No

Under the menu point *User Firewall*, firewall rules can be defined and assigned to specific external users.

By clicking **Yes**, you specify that the firewall rules for the listed users are to be activated as soon as the corresponding user logs in.

Enable group authentication: Yes / No

This function simplifies the user administration for the user firewall, as individual firewall user do not have to be registered with the mGuard anymore.

When a firewall user is configured for RADIUS-Authentication and he authenticates at the mGuard, the RADIUS server will confirm the access by sending an "Access Accept" reply.

With group authentication enabled, the user can also authenticate at the mGuard, even when his name is not defined on the mGuard.

In this case the authentication happens as follows: The user authenticates with the unknown username/password combination and because of group authentication being enabled, the mGuard forwards the request to the RADIUS server. If the RADIUS server confirms the users authentication, it will reply with an "Access Accept" data packet which will also contain a "Filter-ID" attribute containing a group name. This group name will then be used by the mGuard to enable user templates containg the group name as a user firewall template user name.

User Name

Name of the user

Authentication method: Radius / Local

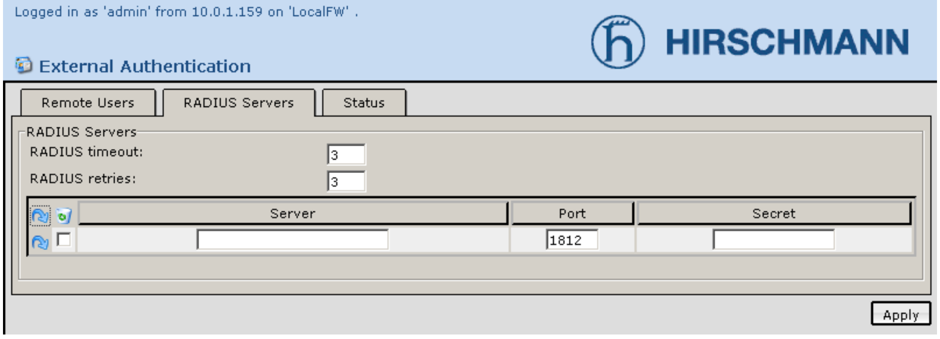
Local:

In the column *User Password*, the password must be entered that has been assigned to the user

Radius:

If a user logs in under his or her password, the mGuard transmits the password entered to the radius server for verification. If the verification is positive, the user will gain access.

Radius Server



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

External Authentication

RADIUS Servers

RADIUS timeout: 3

RADIUS retries: 3

Server	Port	Secret
	1812	

Radius Server

Radius Timeout

Specifies (in seconds) how long the mGuard will wait for the answer from the radius server. Default: 3 (seconds)

Radius retries:

Specifies how often repeat requests will be made to the radius server after a radius timeout has occurred. Default: 3

Server

Name of the server or IP address

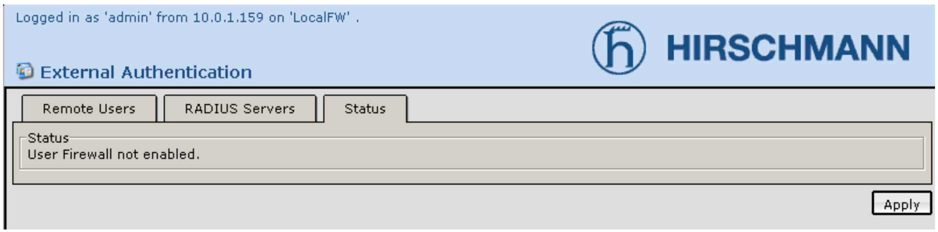
Port

The port number used by the radius server

Secret

Server password

Status



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

External Authentication

Status

User Firewall not enabled.

If the user firewall is activated, its status will be displayed here.

6.4 Menu Network Security (not blade controller)

6.4.1 Network Security → Packet Filter

The mGuard has an integrated *Stateful Packet Inspection Firewall*. The connection data for each active connection is collected in a database (connection tracking). Therefore, it is only necessary to define rules for one direction – data from a connection's other direction – and only this will be automatically passed through. A side-effect is that (when reconfiguring) existing connections will not be dropped even if a corresponding new connection may not be setup.

Factory settings for the packet filter:

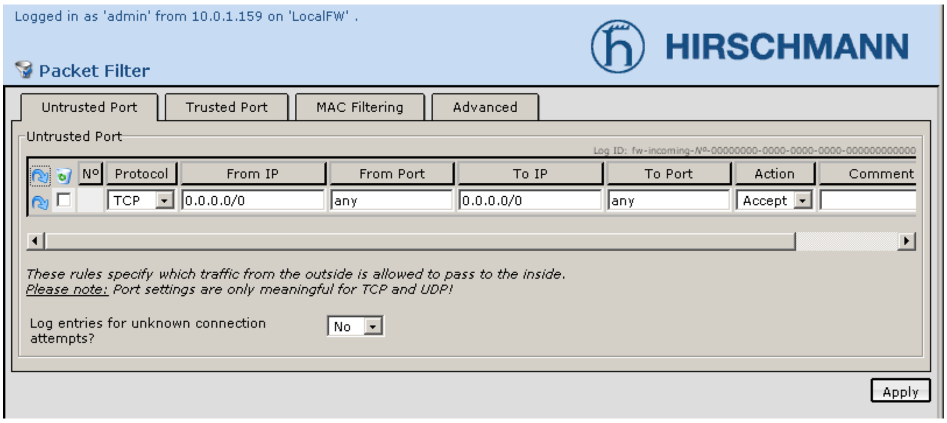
- All incoming connections will be rejected (except VPN).
- The data packets of all outgoing connections will be passed through.

⌦VPN connections are not subject to the firewall rules defined in this menu. You can define firewall rules for each individual VPN connection in the **IPsec VPN → Connections** menu.

⌦The anti-virus function (see "AntiVirus → HTTP" on page 111, "Web Security → FTP" on page 113, "AntiVirus → POP3" on page 116, "AntiVirus → SMTP" on page 119) has priority over the firewall rules defined here and can partially override them. This behaviour can be overridden in the **Network security →** Packet filters, **Extended settings menu** by setting the switch to **Connections scanned for viruses are subject to firewall rules** – see "Extended settings", "Anti-virus scanner" on page 103.

⌦If multiple firewall rules are set, they will be searched in the order in which they are listed (from top to bottom) until a suitable rule is found. This rule will then be applied. If further down in the list there are other rules, which would also fit, they will be ignored.

Untrusted Port



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Packet Filter

Untrusted Port

Log ID: fw-incoming-Nº-00000000-0000-0000-0000-000000000000

		Nº	Protocol	From IP	From Port	To IP	To Port	Action	Comment
	□		TCP	0.0.0.0/0	any	0.0.0.0/0	any	Accept	

These rules specify which traffic from the outside is allowed to pass to the inside.
Please note: Port settings are only meaningful for TCP and UDP!

Log entries for unknown connection attempts? No

Untrusted Port

Lists the firewall rules that have been set. These rules apply for incoming data connections, i.e. ones which were initiated by an external system.

If no rule has been set, all incoming connections (except VPN) will be dropped (= factory setting).

You have the following options for the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

IP address

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets are passed through.

Reject means that the data packets are rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, Reject has the same effect as Drop (see below).)

Drop means that the data packets are not passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

⌧ In Transparent mode, **Reject** is not supported.

Comment

An informational comment for this rule.

Log

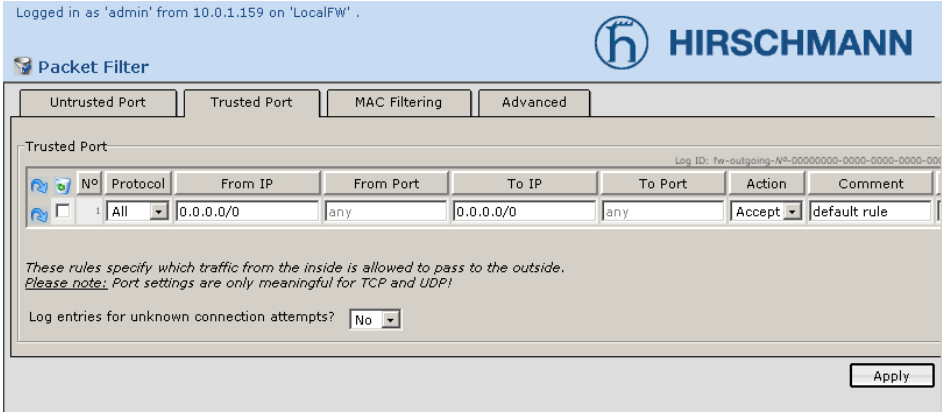
You can specify - for each individual firewall rule - whether the use of the rule

- ☞ should be logged by setting - *Log* to **Yes**
- ☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

Trusted Port



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Packet Filter

Trusted Port

Log ID: fw-outgoing-Nº-00000000-0000-0000-0000-00

	Nº	Protocol	From IP	From Port	To IP	To Port	Action	Comment
☐	1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule

These rules specify which traffic from the inside is allowed to pass to the outside.
Please note: Port settings are only meaningful for TCP and UDP!

Log entries for unknown connection attempts? No

Trusted Port

Lists the firewall rules that have been set. These rules apply for outgoing connections; i.e. ones which were initiated internally to communicate with a remote site.

The default (factory) setting is a rule that allows all outgoing connections.

If no rule is set, all outgoing connections are forbidden (except VPN).

You have the following options for the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

IP address

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets are passed through.

Reject means that the data packets are rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, Reject has the same effect as *Drop* (see below).)

Drop means that the data packets are not passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

⌦ In Transparent mode, **Reject** is not supported.

Comment

An informational comment for this rule.

Log

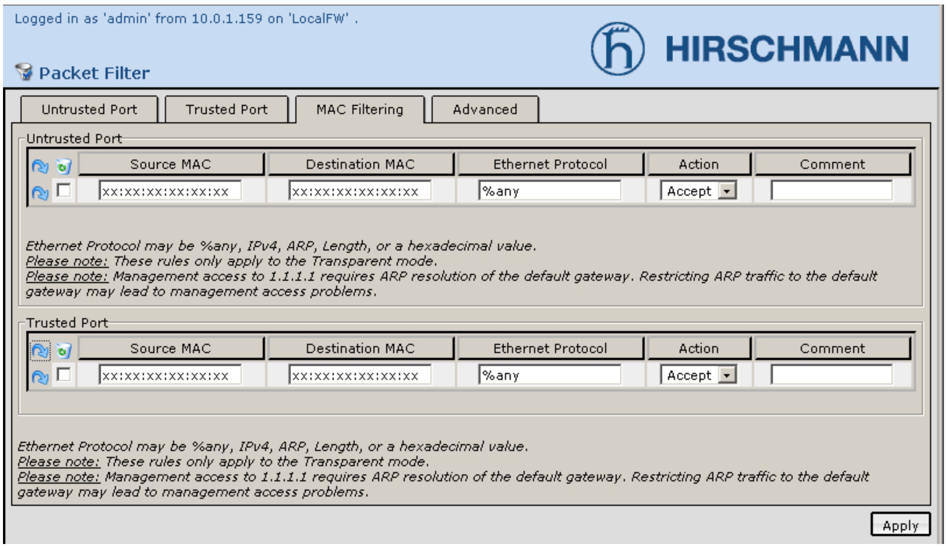
You can specify - for each individual firewall rule - whether the use of the rule

- ☞ should be logged by setting - *Log* to **Yes**
- ☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

MAC Filter



Untrusted Port

Source MAC	Destination MAC	Ethernet Protocol	Action	Comment
xx:xx:xx:xx:xx:xx	xx:xx:xx:xx:xx:xx	%any	Accept	

Ethernet Protocol may be %any, IPv4, ARP, Length, or a hexadecimal value.
Please note: These rules only apply to the Transparent mode.
Please note: Management access to 1.1.1.1 requires ARP resolution of the default gateway. Restricting ARP traffic to the default gateway may lead to management access problems.

Trusted Port

Source MAC	Destination MAC	Ethernet Protocol	Action	Comment
xx:xx:xx:xx:xx:xx	xx:xx:xx:xx:xx:xx	%any	Accept	

Ethernet Protocol may be %any, IPv4, ARP, Length, or a hexadecimal value.
Please note: These rules only apply to the Transparent mode.
Please note: Management access to 1.1.1.1 requires ARP resolution of the default gateway. Restricting ARP traffic to the default gateway may lead to management access problems.

Beside the IP firewall (OSI Layer 3/4), which filters ICMP messages and TCP/UDP connections, the mGuard, when operating in Transparent mode, can additionally filter for MAC addresses and ethernet protocols (OSI Layer 2).
In contrast to the IP firewall, the MAC filter is stateless. This means an additional rule must be created for some rules in the opposite direction where necessary.

When no rules are defined, all ARP and IP frames are allowed.

☒ Please note the annotations on the screen when you define MAC filtering rules.
☒ Rules defined here supersede the IP firewall rules.

Source MAC

Definition of the source MAC address. **xx:xx:xx:xx:xx:xx** is a wildcard for all MAC addresses.

Destination MAC

Definition of the destination MAC address. **xx:xx:xx:xx:xx:xx** is a wildcard for all MAC addresses. The values **ff:ff:ff:ff:ff:ff** is the broadcast MAC address, to which, for example, all ARP requests are being sent.

Ethernet Protocol

%any is a wildcard for all ethernet protocols. Protocols can be specified by name or hexadecimal value, for example:

- IPv4 or 0800
- ARP or 0806

Action

Accept means that frames can pass.

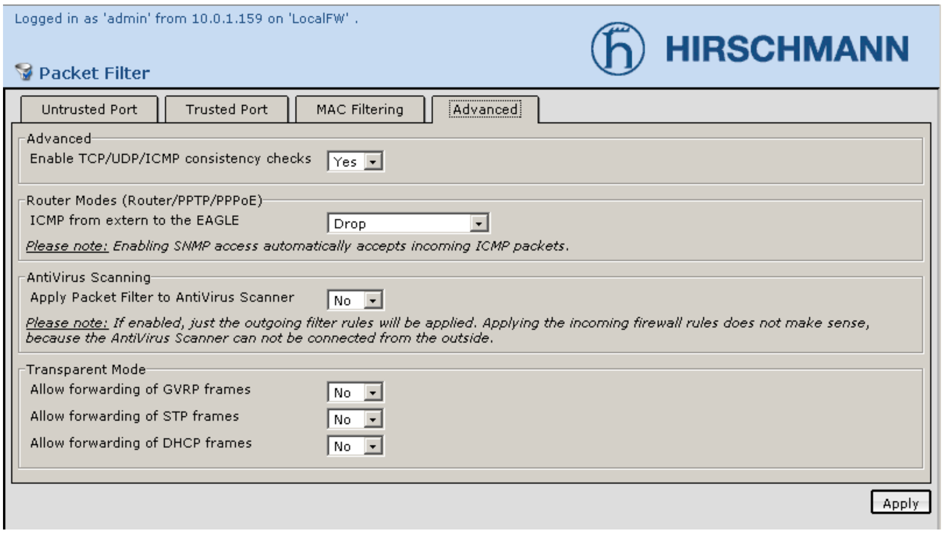
Drop means to drop frames.

Comment

An informational comment for this rule.

☞ The MAC filter does not support logging.

Advanced



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Packet Filter

Advanced

Enable TCP/UDP/ICMP consistency checks: Yes

Router Modes (Router/PPTP/PPPoE)

ICMP from extern to the EAGLE: Drop

Please note: Enabling SNMP access automatically accepts incoming ICMP packets.

AntiVirus Scanning

Apply Packet Filter to AntiVirus Scanner: No

Please note: If enabled, just the outgoing filter rules will be applied. Applying the incoming firewall rules does not make sense, because the AntiVirus Scanner can not be connected from the outside.

Transparent Mode

Allow forwarding of GVRP frames: No

Allow forwarding of STP frames: No

Allow forwarding of DHCP frames: No

The settings affect the basic behavior of the firewall.

Advanced

Enable TCP/UDP/ICMP consistency checks

When set to **Yes** the mGuard performs various checks for wrong check sums, packet sizes, etc. and drops packets failing the check.
The factory default for this option is **Yes**.

Router Modes (Router/PPTP/PPPoE)

ICMP from extern to the mGuard

With this option you can control which ICMP messages from the external network are accepted by the mGuard. You have the following options:

Drop: All ICMP-messages sent to the mGuard from the external network will be dropped.

Allow ping requests: Only ping requests (ICMP message type 8) from the external network will be accepted.

Allow all ICMPs: All ICMP messages from the external network will be accepted.

Anti-virus scanner

Connections scanned for viruses are subject to firewall rules: Yes / No

In the *AntiVirus →HTTP, AntiVirus → FTP, AntiVirus→ POP3, AntiVirus →SMTP* menus, a list of server connections can be created on the *Anti-virus protection* tab. Files that enter mGuard via these connections are scanned for viruses (in the case of SMTP, outgoing mGuard files) .

If firewall packet filters are set (Network security →Packet filters and/or Network security → User firewall) which relate to these connections and prevent them, these will only be taken into consideration if the **Connections scanned for viruses are subject to firewall rules** switch is set to Yes. In the case of No (= default setting), the rules that have been set for the anti-virus function have priority. Firewall packet filters that contradict them are overridden.

VPN connections are not affected because the anti-virus function is not available for VPN connections.

Transparent Mode

Allow forwarding of GVRP frames

The GARP VLAN Registration Protocol (GVRP) is used by GVRP capable switches to exchange configuration information.

By setting this switch to **Yes**, GVRP frames are allowed to traverse the mGuard in Transparent Modus.

Allow forwarding of STP frames

The Spanning-Tree Protocol (STP) (802.1d) is used by bridges and switches to detect and avoid loops in the network topology.

By setting this switch to **Yes**, STP frames are allowed to traverse the mGuard in Transparent Modus.

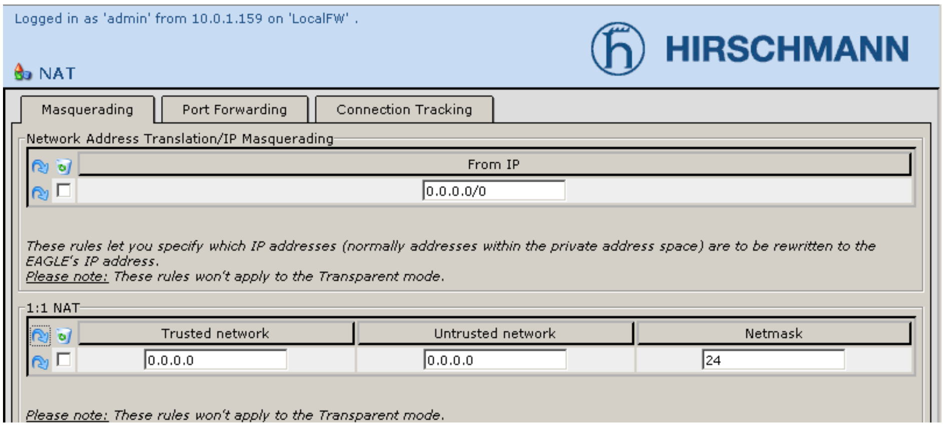
Allow forwarding of DHCP frames

Allow the client to retrieve an IP address using DHCP independently from the outgoing firewall rules.

This switch is set to **Yes** per default.

6.4.2 Network Security → NAT

Masquerading



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

NAT

Network Address Translation/IP Masquerading

	From IP
□	0.0.0.0/0

These rules let you specify which IP addresses (normally addresses within the private address space) are to be rewritten to the EAGLE's IP address.
Please note: These rules won't apply to the Transparent mode.

1:1 NAT

	Trusted network	Untrusted network	Netmask
□	0.0.0.0	0.0.0.0	24

Please note: These rules won't apply to the Transparent mode.

Network Address Translation/IP Masquerading

Lists the rules set for NAT (**N**etwork **A**ddress **T**ranslation).

In the case of outgoing data packets, the device can translate the sender‘s IP address (From IP) in the trusted network to the device‘s own external address. This technique is called NAT (Network Address Translation).

This method is used whenever the internal address cannot or should not be routed externally, e.g. since it is in a private address space such as 192.168.x.x or because you wish to keep the internal network structure hidden.

This method is also called *IP-Masquerading*.

⌦ If the mGuard is in *PPPoE/PPTP* mode, NAT must be activated to enable access to the Internet. If NAT is not activated, the device will only allow VPN connections.

⌦ When using more than one IP address for an interface, always the first IP address of the list will be used for IP-Masquerading.

⌦ These rules don’t apply to the Transparent mode.

Factory setting: NAT is not active.

You have the following options for the entries:

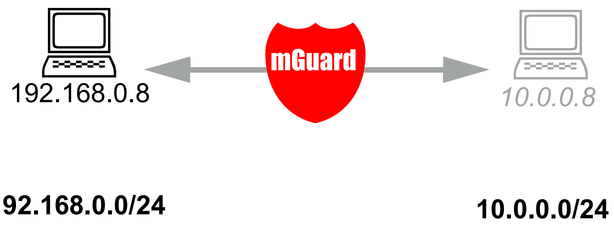
From IP

0.0.0.0/0 means all addresses, i.e. all internal IP addresses will be translated using NAT. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

1:1 NAT

Lists the rules set for 1:1 NAT (**N**etwork **A**ddress **T**ranslation), which mirrors addresses from the internal (trusted) network into the external network.

In the following example the mGuard is inside the net 192.168.0.0/24 with its internal interface and inside the net 10.0.0.0/24 with its external interface. By using 1:1 NAT, the computer with the IP 192.168.0.8 can be reached under the IP 10.0.0.8 in the external network.



☒ These rules don’t apply to the Transparent mode.

Factory setting: NAT is not active.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 44.

You have the following options for the entries:

Trusted network

The network address on the local interface (LAN).

Untrusted network

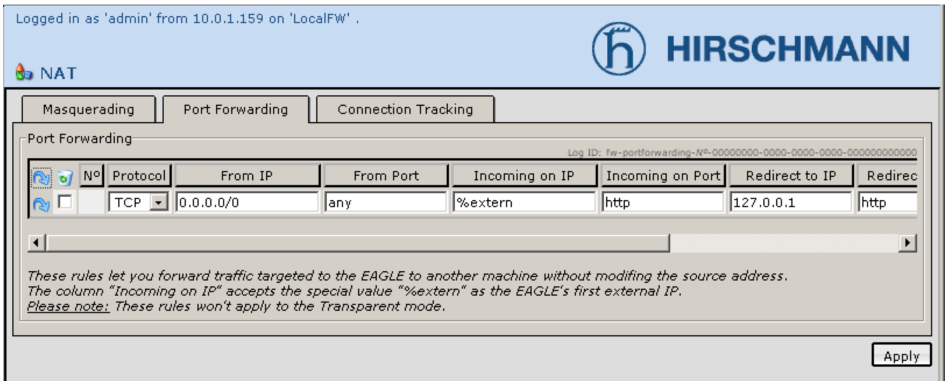
The network address on the external interface (WAN).

Netmask

The network mask as a value between 1 and 32 for the local and external network address. (See also: “CIDR (Classless InterDomain Routing)” on page 140.)

Port Forwarding

.



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Port Forwarding

Log ID: fw-portforwarding-Nº-00000000-0000-0000-0000-000000000000

		Nº	Protocol	From IP	From Port	Incoming on IP	Incoming on Port	Redirect to IP	Redirec
	□		TCP	0.0.0.0/0	any	%extern	http	127.0.0.1	http

These rules let you forward traffic targeted to the EAGLE to another machine without modifing the source address.
The column “Incoming on IP” accepts the special value “%extern” as the EAGLE’s first external IP.
Please note: These rules won’t apply to the Transparent mode.

Apply

Lists the rules set for port forwarding.
Port forwarding performs the following: The headers of data packets incoming

from the external network, which are addressed to the mGuard's external IP address (or one of its external IP addresses) and to one of the ports on the mGuard, will be rewritten to forward them to a specific port on a specific system in the internal network. In other words, both the IP address and the port number (in the header of the incoming data packets) will be changed.
This method is also called Destination NAT.

⌦The rules set here have priority over the settings made in the **Network Security Packet Filter → Untrusted Port** menu.
⌦These rules don't apply to the Transparent mode.

Protocol
Specify the protocol which the rule should govern.

From IP
The source IP for which forwarding shall be performed.

From Port
The source port for which forwarding shall be performed.

any specifies any port.

Ports may be either port numbers or services names, like *pop3* for port 110 or *http* for port 80.

Incoming on IP
Enter the external IP address (or one of the external IP addresses) of the mGuard here.

OR

If the destination IP address of the mGuard is assigned dynamically, this cannot be specified. In this case, use the following variable: **%extern**

⌦The variable „%extern" always corresponds to the first IP address of the address list, when using more than one static IP address.

Incoming on Port
The original destination port of the incoming data packets must be given in this field.

Redirect to IP
In this field, enter the internal IP address to which the data packets should be forwarded. The original destination address will be overwritten with the address entered in this field.

Redirect to Port
In this field, enter the port to which the data packets should be forwarded. The original entry for the destination port will be overwritten with the port specified in this field.

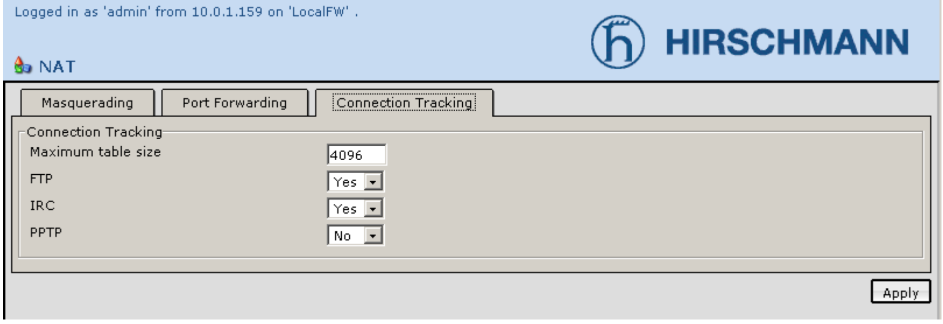
Comment
An informational comment for this rule.

Log
You can specify - for each individual port forwarding rule - whether the use of the rule

☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Connection Tracking


Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Maximum table size 4096
FTP Yes
IRC Yes
PPTP No

Connection Tracking

Maximum table size

This entry specifies an upper limit for maximum number of connections being tracked.

The default setting is selected in such a way that it is never reached under normal conditions. During attacks it may be easily reached so that this limit provides an additional protection. If special requirements should be present in your operating environment, then you can increase this value.

FTP

If an outgoing FTP (protocol) connection is setup to download data, there are two alternatives as to how the data will be transmitted: When using “active FTP” the server called will call the calling system back to establish a connection for the transfer of data. When using “passive FTP” the calling system will establish this additional connection for the data transfer. To let the data of this additional connection pass through the firewall, **Enable “FTP” NAT/Connection Tracking support** must be set to **Yes** (factory setting).

IRC

This is similar to “FTP”: When the IRC protocol is used for chatting in the Internet, incoming connections must also be permitted after the connection has been established actively. In this case, **Enable “IRC” NAT/Connection Tracking support** must be set to **Yes** so that the firewall will permit these connections (factory setting).

PPTP

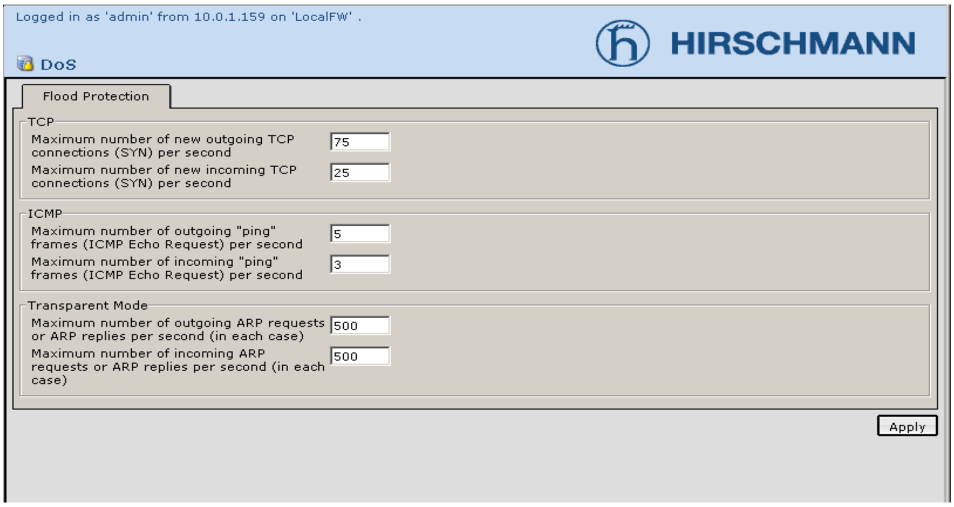
This need only be set to **Yes** under the following condition:

if a local system should establish a VPN connection via PPTP to an external system without help from the mGuard.

The factory setting is **No**.

6.4.3 Network Security → DoS

Flood Protection



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

DoS

Flood Protection

TCP

Maximum number of new outgoing TCP connections (SYN) per second: 75

Maximum number of new incoming TCP connections (SYN) per second: 25

ICMP

Maximum number of outgoing "ping" frames (ICMP Echo Request) per second: 5

Maximum number of incoming "ping" frames (ICMP Echo Request) per second: 3

Transparent Mode

Maximum number of outgoing ARP requests or ARP replies per second (in each case): 500

Maximum number of incoming ARP requests or ARP replies per second (in each case): 500

TCP

Maximum number of new outgoing TCP connections (SYN) per second
Default: 75

Maximum number of new incoming TCP connections (SYN) per second

Default: 25

These 2 settings define upper limits for the allowed incoming and outgoing TCP connections per second. The default values will never be reached in normal operation. However, since they can be easily reached in the event of an attack, the limits provide additional security. If your operational environment has special requirements, you can increase these values.

ICMP

Maximum number of outgoing ’ping’ frames (ICMP Echo Request) per second
Default: 5

Maximum number of incoming ’ping’ frames (ICMP Echo Request) per second
Default: 3

These 2 settings define upper limits for the allowed incoming and outgoing ping frames per second. The default values will never be reached in normal operation. However, since they can be easily reached in the event of an attack, the limits provide additional security. If your operational environment has special requirements, you can increase these values.

Transparent Mode

Maximum number of outgoing ARP requests or ARP replies per second (in each case)
Default: 500

Maximum number of incoming ARP requests or ARP replies per second (in each case)
Default: 500

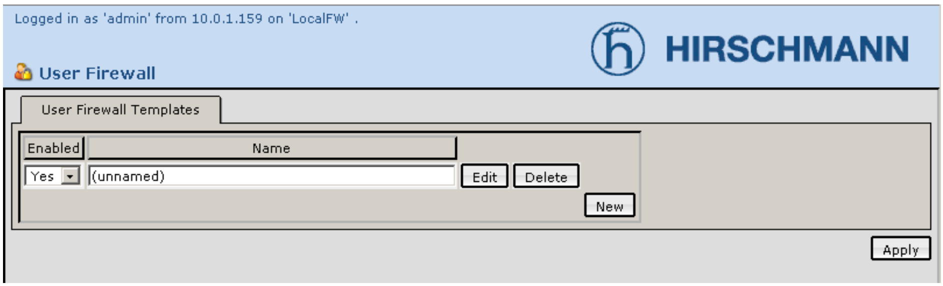
These 2 settings define upper limits for the allowed incoming and outgoing ARP requests and ARP replies per second. The default values will never be reached in normal operation. However, since they can be easily reached in the event of an attack, the limits provide additional security. If your operational environment has special requirements, you can increase these values.

6.4.4 Network Security → User Firewall

The user firewall is operative exclusively for firewall users, i.e., users that registered as firewall users – see “Security → External Authentication” on page 83. A set of firewall rules, a so-called template, can be assigned to each firewall user.

⌧ The anti-virus function (see “AntiVirus → HTTP” on page 111, ““Web Security → FTP” on page 113, “AntiVirus → POP3” on page 116, “AntiVirus → SMTP” on page 119) has priority over the firewall rules defined here and can partially override them. This behaviour can be overridden in the **Network security → Packet filters**, Extended Settings menu by setting the switch to **Connections scanned for viruses are subject to firewall rules** – see “Advanced”, “Anti-virus scanner” on page 89.

User Firewall Templates


Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Enabled	Name
Yes	(unnamed)

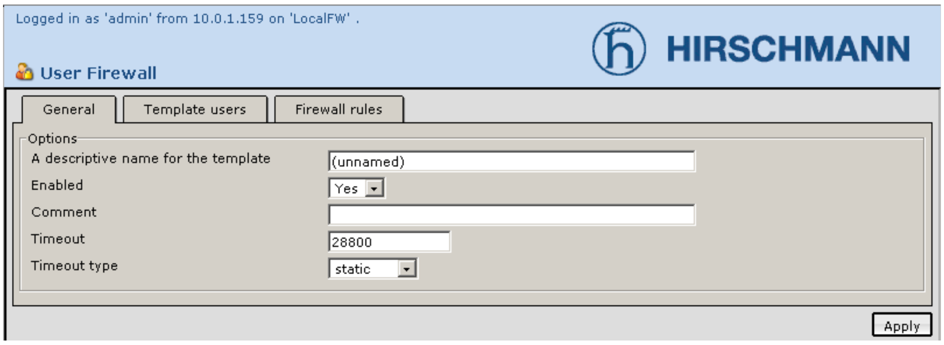
All defined user firewall templates are listed here. A template can consist of several firewall rules. A template can be assigned to several users.

- **Enabling / Disabling a defined user firewall templat**e:
  Set Parameters active to Yes or No, respectively.
- **Editing a defined user firewall template:**
  Click the Edit button next to the list entry.
- **Deleting a defined user firewall template:**
  Click the Delete button next to the list entry.
- **Defining a new user firewall template**:
  1. Click the **New** button.
     Result: the list of user firewall templates displayed will be supplemented with a new entry.
  2. Next to the list entry, click the **Edit** button.

User Firewall → Define Template

General:

After clicking on the **Edit** button, the following page will appear:



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

User Firewall

Options

A descriptive name for the template: (unnamed)

Enabled: Yes

Comment:

Timeout: 28800

Timeout type: static

Options

A descriptive name for the template

You can name or rename the user template as desired.

Active: Yes / No

For **Yes**, the user firewall template becomes active as soon as external users log onto the mGuard who are listed on the *Template User* register card (see below) and who have been assigned firewall rules. It doesn't matter from which computer and under which IP address the user logs in. The assignment of user firewall rules is based on the authentication data that the user enters during the login (user name, password).

Comments

Optional: explanatory text

Timeout

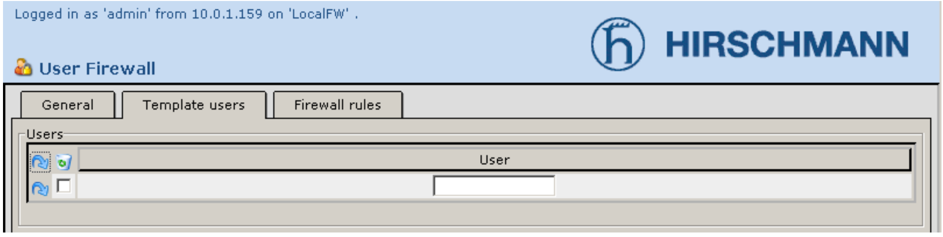
Default: 28800.

Indicates the time in seconds at which point the firewall rules will be deactivated. If the user session lasts longer than the timeout time defined here, the user will have to repeat the login process.

Timeout type: static / dynamic

With static timeout users are logged out automatically, as soon as the specified timeout elapsed. With dynamic timeout users are logged out automatically after a period of inactivity has elapsed.

Template User



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

User Firewall

Users

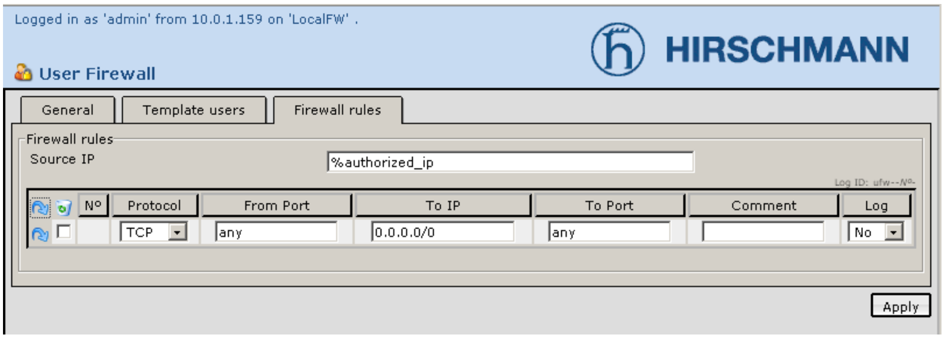
	User
□	

Users

User Name

Enter the names of users here. The names must correspond to those that have been defined in Security → External Authentication - for more information, see "Security → External Authentication" on page 83

Firewall Rules



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

User Firewall

Firewall rules

Source IP: %authorized_ip

N°	Protocol	From Port	To IP	To Port	Comment	Log
☐	TCP	any	0.0.0.0/0	any		No

Firewall Rules

Source IP

The IP address from which the user connected to the mGuard. “%authorized_ip” is a placeholder for the address.

⌧ If several firewall rules have been defined and activated for a single user, these will be queried in sequence from top to bottom, until the appropriate rule has been located. This rule will then be applied. If further rules are defined in the rule list that would also be suitable, these are ignored.

You are offered the following options for entries:

Protocol

All encompasses: TCP, UDP, ICMP and other IP protocols.

From Port/To Port

(is only evaluated for the TCP and UDP protocols)

Any designates any port.

Startport:Endport (e.g. 110:120) designates a port range.

Individual ports can be entered either using the port number or the corresponding service names: (e.g. 110 for pop3 or pop3 for 110).

To IP

0.0.0.0/0 means all IP addresses. In order to specify an IP-address range, use CIDR notation - see e “CIDR (Classless InterDomain Routing)” on page 140.

Comment

A comment can be entered as desired for this rule.

Log

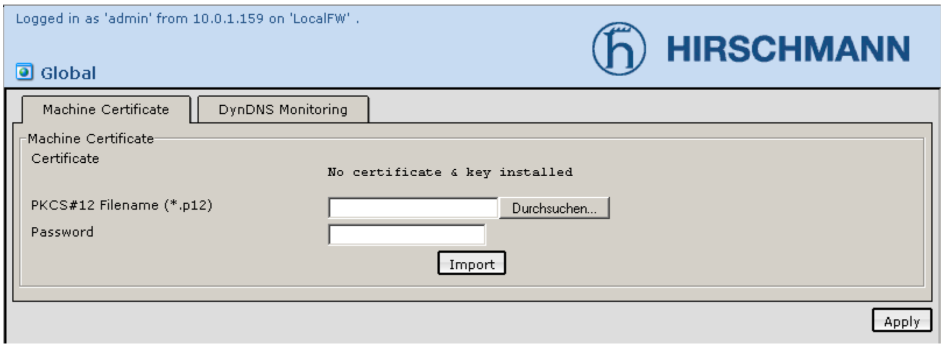
For each individual firewall rule, you may define whether, once the rule is activated

- the event should be logged - set *Log* to **Yes**
- or not - set *Log* to **No** (default setting).

6.5 Menu IPsec VPN (not blade controller)

6.5.1 IPsec VPN → Global

Machine Certificate



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Machine Certificate

Certificate: No certificate & key installed

PKCS#12 Filename (*.p12):

Password:

Machine Certificate

This shows the currently imported X.509 certificate with which the mGuard identifies itself to other VPN gateways. The following information is displayed:

subject	The holder to whom the certificate was issued.
issuer	The certification authority which signed the certificate. C: Country ST: State L: Location (city) O: Organisation OU: Organisation Unit CN: Common Name (hostname)
MD5, SHA1 Fingerprint	Fingerprint of the certificate to compare this with another person, e.g. on the telephone. Windows displays the fingerprint in SHA1 format here.
notBefore, notAfter	Period of time that the certificate is valid. This is ignored by the mGuard, since it doesn't have an integrated realtime clock.

In addition to the information given above, the imported PKCS#12 file (filename extension *.p12 or *.pfx) also contains a public and a private key. The public key will be given in as a certificate file (filename extension *.cer or *.pem) to other VPN gateways and is used to verify that this machine owns the corresponding private key.

Depending on the respective remote site, its operator must be supplied with the certificate file in person or via a signed e-mail or if a secure means of communication is not available, you should conclude by comparing the fingerprint shown by the mGuard via a secure means.

Only one PKCS#12 file can be imported into the device.

To import a (new) certificate, proceed as follows:

Import a new certificate

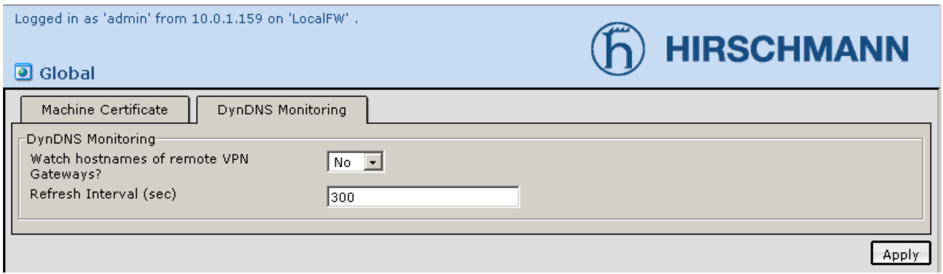
Prerequisite:

The PKCS#12 file (filename = *.p12 or *.pfx) is generated and saved on the connected system.

1. Click on **Browse...** to select the file.
2. Enter the password with which the PKCS#12 file's private key is protected in the *Password* field.

3. Click on **Import**.
4. Then click on **OK**.
   After the import is completed, the new certificate will be shown under *Certificate*.

DynDNS Monitoring



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Global

Machine Certificate | DynDNS Monitoring

DynDNS Monitoring

Watch hostnames of remote VPN Gateways? No

Refresh Interval (sec) 300

Apply

For an explanation of DynDNS, see below: Services → DynDNS Registration.

Watch hostnames of remote VPN Gateways? Yes / No

If the mGuard has been given the address of the remote VPN gateway as a hostname (see “Connections” on page 99) and this hostname has been registered with a DynDNS Service, the mGuard can check against the DynDNS at regular intervals whether any changes have occurred. If yes, the VPN connection will be setup to the new IP address.

Refresh Interval (sec)

Standard: 300 (seconds)

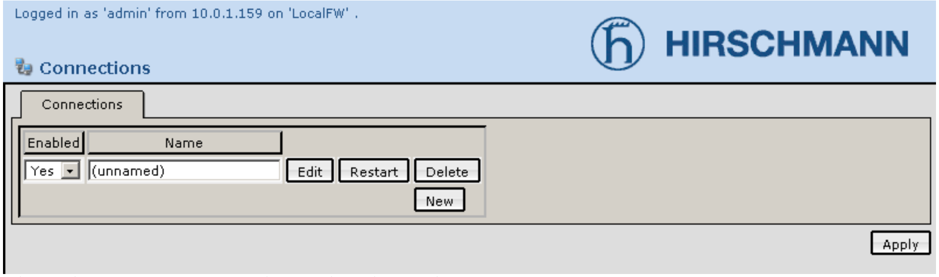
6.5.2 IPsec VPN → Connections

Prerequisites for a VPN connection:

The main prerequisite for a VPN connection is that the IP addresses of the VPN partner are known and accessible.

- In order for an IPsec connection to be setup successfully, the VPN’s remote site must support IPsec with the following configuration:
  – Authentication via Pre-Shared Key (PSK) or X.509 certificate
  – ESP
  – Diffie-Hellman Groups 2 and 5
  – DES, 3DES or AES encryption
  – MD5 or SHA-1 hash algorithms
  – Tunnel or Transport mode
  – Quick Mode
  – Main Mode
  – SA Lifetime (1 second to 24 hours)
  If the system at the remote site is running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least *Service Pack 2* must be installed.
- If the remote site is behind a NAT router, it must support NAT-T. Or the NAT router must support the IPsec protocol (IPsec/VPN Passthrough). In either case, for technical reasons, only IPsec Tunnel connections are supported.

Connections



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Connections

Connections

Enabled	Name			
Yes	(unnamed)	Edit	Restart	Delete
				New

Apply

Lists the VPN connections that have been set up.

- **VPN connections - enable / disable**
  You can activate (Enable = **Yes**) or deactivate (Enable = **No**) each individual connection.
- **VPN connections - editing**
  Click on the **Edit** button next to the entry.
  Make the necessary or desired settings (see below).
  Then click on **OK**.
- **VPN connections - deleting**
  Click on the **Delete** button next to the entry.
  Then click on **OK**.
- **Configuring a new VPN connection**
  Click on **New**.
  Enter a name for the connection and then click on **Edit.**
  Make the necessary or desired settings (see below).
  Then click on **OK**.

To enable or disable VPN connections from remote, connect to the mGuard using the following URLs:

`https://`*login*`:`*password*`@`*host*`/nph-vpn.cgi?name=`*Connection*`&cmd=`*(*`up|down`*)*

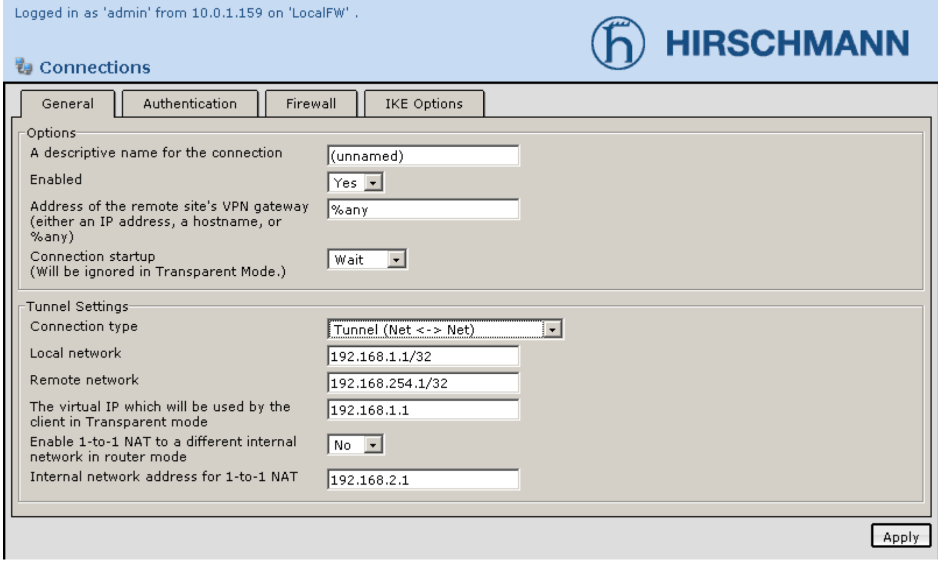
Example:

```
https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=paris&cmd=up
```

6.5.3 Define a VPN connection

After pressing the **Edit** button, the following page appears

General



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Options

A descriptive name for the connection	(unnamed)
Enabled	Yes
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	%any
Connection startup (Will be ignored in Transparent Mode.)	Wait

Tunnel Settings

Connection type	Tunnel (Net <-> Net)
Local network	192.168.1.1/32
Remote network	192.168.254.1/32
The virtual IP which will be used by the client in Transparent mode	192.168.1.1
Enable 1-to-1 NAT to a different internal network in router mode	No
Internal network address for 1-to-1 NAT	192.168.2.1

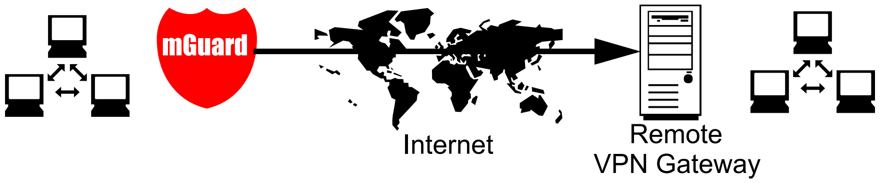
Options

A descriptive name for the connection
You can assign the connection any name you desire.

Enabled
Specify whether the connection should be enabled (= Yes) or not (= No).

Address of the remote site’s VPN gateway

(An IP address, a hostname or %any)



The address of the gateway to the private network in which the remote communication partner can be found.

– If you wish to have the mGuard actively initiate and set up the connection to the remote site or if the device is in *Transparent* mode, enter the IP address or the hostname of the remote site here.

– If the remote site’s VPN gateway does not have a fixed and known IP address, you can use the DynDNS Service to simulate a fixed and known address. See “DynDNS” on page 132.

– If you want the mGuard to be ready to accept a connection actively initiated and set up by a remote site with any IP address, enter: **%any**

– In this case, the local mGuard can be “called” by a remote site, which has been dynamically assigned its IP address (by the internet service provider), which has an IP address that changes. In this scenario, you may only enter an IP address when this is the fixed and known IP address of the remote “calling” site.

☒ **%any** can only be used along with the authentication mode using X.509 certificates.

☒ In case the remote peer is located behind a NAT gateway, **%any** must be used. Otherwise the renegotiation of new connection keys will fail after the connection is established.

Connection startup

There are 2 options:

- Start a connection to the remote side
- Wait for the remote side [to setup a connection]

Start a connection to the remote side

In this case, the local mGuard sets up the connection to the remote side. The fixed IP address or domain name of the remote side must be entered in the *Address of the remote site‘s VPN gateway* (see above) field.

Wait for the remote side [to setup a connection]

In this case, the local mGuard is ready to accept a connection, which a remote site actively initiates and sets up to the local mGuard. The entry in the *Address of the remote site‘s VPN gateway* (see above) field may be: **%any**

☞ If the mGuard should only accept a connection initiated by a specific remote site (which has a fixed IP address), you can enter its IP address or hostname just to be on the safe side.

☞ If the mGuard is running in *Transparent* mode, this setting has no effect. In other words, it will be ignored and the connection will be initiated automatically, whenever the mGuard notices that the connection should be used.

Tunnel Settings

Connection type

You can choose from:

- Tunnel (Net[work] ←→ Net[work])
- Transport (Host ←→ Host)
- Transport (L2TP Microsoft Windows)
- Transport (L2TP SSH Sentinel)

Tunnel (Net[work] ←→ Net[work])

This type of connection is not only suitable in every case, but also the most secure. In this mode, the IP datagrams are completely encrypted before they are sent with a new header to the remote site's VPN gateway – the "tunnel end". There the transferred datagrams are decrypted to restore the original datagrams. These are then passed on to the destination system.

Transport (Host ←→ Host)

In this type of connection, the device only encrypts the data of the IP packets. The IP header information remains unencrypted.

Transport (L2TP Microsoft Windows)

If this type of connection is activated, the mGuard will use a transport connection which is compatible with the IPsec/L2TP client available in older Microsoft Windows systems.

If you select this option you should also set *Perfect Forward Secrecy (PFS)* to **No** and enable the L2TP server.

Transport (L2TP SSH Sentinel)

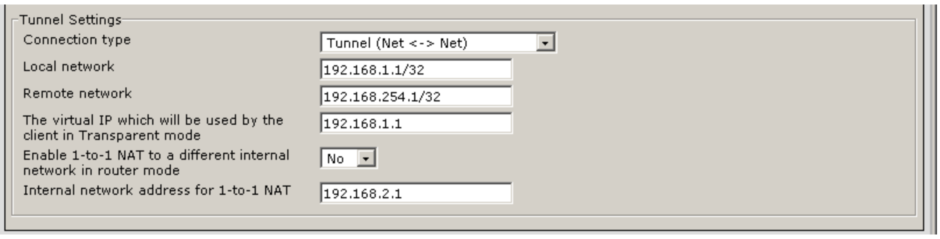
If this type of connection is activated, the mGuard will use a transport connection which is compatible with the IPsec/L2TP client available in recent Microsoft Windows systems and the SSH Sentinel VPN client.

If you select this option you should also set *Perfect Forward Secrecy (PFS)* to **No** (see below) and enable the L2TP server.

☞ As soon as the IPsec/L2TP connection is started under Windows, a dialog will appear to prompt you to enter your user name and login. You can make any entry that you want in this dialog. Since the X.509 certificate has already provided your authentication, the mGuard will ignore these entries.

Tunnel Settings, with Connection Type Tunnel (Net <-> Net)

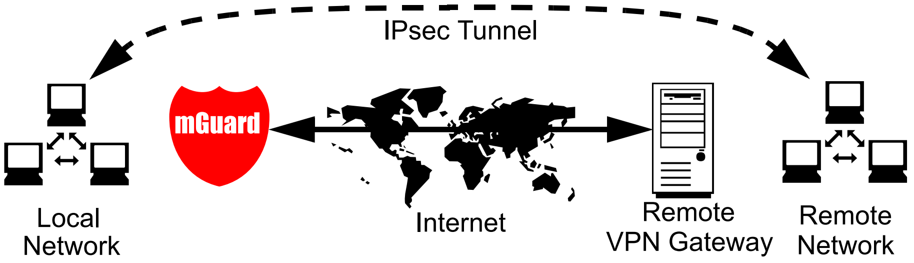
When the Connection Type is set to "Tunnel", the following entries appear on the page:



Tunnel Settings

Connection type	Tunnel (Net <-> Net)
Local network	192.168.1.1/32
Remote network	192.168.254.1/32
The virtual IP which will be used by the client in Transparent mode	192.168.1.1
Enable 1-to-1 NAT to a different internal network in router mode	No
Internal network address for 1-to-1 NAT	192.168.2.1

Please make the following settings to specify the VPN tunnel:



Local network address

With this entry, you specify the address of the network or computer which is connected to the local interface of the mGuard.

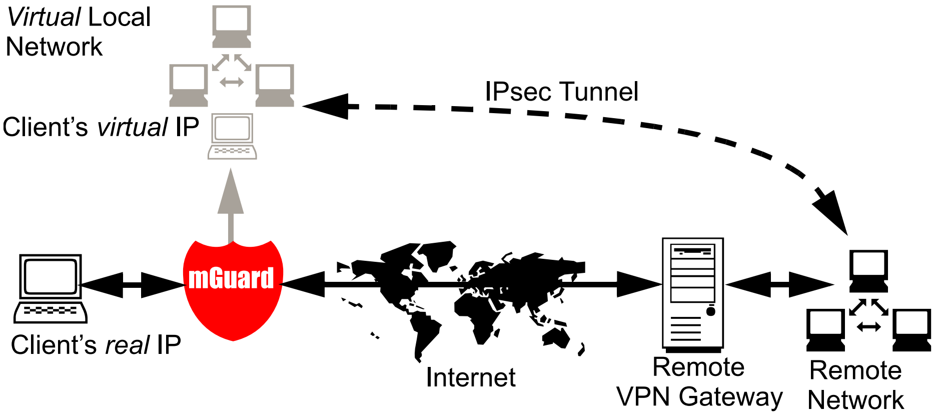
Remote network address

With this entry, you specify the address of the network or computer which is available behind the remote VPN gateway.

☞ The network 0.0.0.0/0 specifies a *default route over the VPN.*

This means that all traffic for which there is no other VPN tunnel or route will be routed through this VPN tunnel.
A default route over VPN should only be specified for a single tunnel and is not available in *Transparent* mode.

The virtual IP which will be used by the Single Client Transparent mode



In *Transparent* mode the VPN's local network is simulated by the mGuard. Inside this *virtual* network, the client will be known under a *virtual IP*.

⌧This entry is only required in *Transparent* mode.

Activate 1-to-1 NAT in another internal network in Router mode: Yes / No

Transcribe the local network defined in the VPN tunnel to a local network available for the local (LAN) Ethernet port.

An explanation for 1-to-1 NAT can be found unde "Network Address Translation/IP Masquerading" on page 90.

Internal network for 1-to-1 NAT

The network address for the local (LAN) Ethernet port. The net mask is taken over from the *local network* field.

Authentication

Authentication method

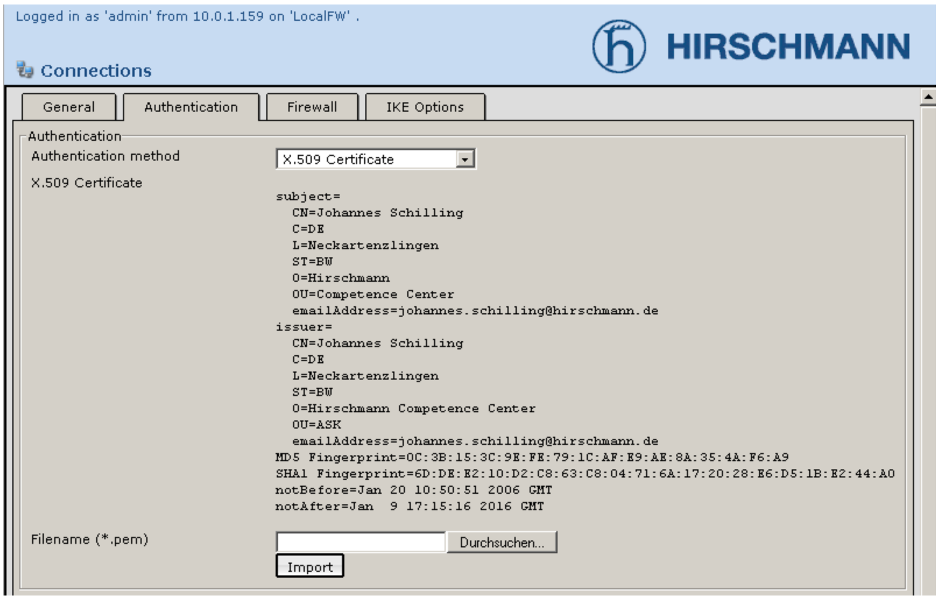
There are 2 options:

– X.509 Certificate

– Pre-Shared Key

Depending on which option you have choosen, the page will present you different possibilities for adjustments:

Authentication method: X.509 Certificate



Authentication

Authentication method: X.509 Certificate

X.509 Certificate

```
subject=
  CN=Johannes Schilling
  C=DE
  L=Neckartenzlingen
  ST=BW
  O=Hirschmann
  OU=Competence Center
  emailAddress=johannes.schilling@hirschmann.de
issuer=
  CN=Johannes Schilling
  C=DE
  L=Neckartenzlingen
  ST=BW
  O=Hirschmann Competence Center
  OU=ASK
  emailAddress=johannes.schilling@hirschmann.de
MD5 Fingerprint=0C:3B:15:3C:9E:FE:79:1C:AF:E9:AE:8A:35:4A:F6:A9
SHA1 Fingerprint=6D:DE:E2:10:D2:C8:63:C8:04:71:6A:17:20:28:E6:D5:1B:E2:44:A0
notBefore=Jan 20 10:50:51 2006 GMT
notAfter=Jan  9 17:15:16 2016 GMT
```

Filename (*.pem)

These methods are supported by most of the newer IPsec implementations. In this case, the mGuard uses the public key of the remote site (filename *.cer or *.pem) to encrypt the authentication datagram before it sends it to the remote site, the “tunnel end”. (You must have received this *.cer or *.pem file from the operator at the remote site – perhaps on a floppy disc or attached to an e-mail).

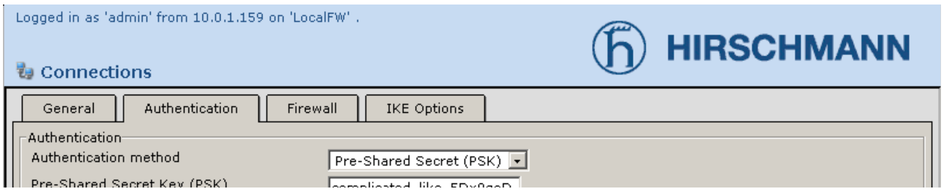
To make this public key available to the mGuard, proceed as follows:

Prerequisite:

The *.cer or *.pem file must have been saved on the configuration system.

1. Click on **Browse...** and select the file.
2. Click on **Import**.
   After the import, the contents of the new certificate will be displayed. An explanation of the information displayed can be found in the chapter “Machine Certificate” on page 98.

Authentication method: Pre-Shared Secret Key (PSK)



Authentication

Authentication method: Pre-Shared Secret (PSK)

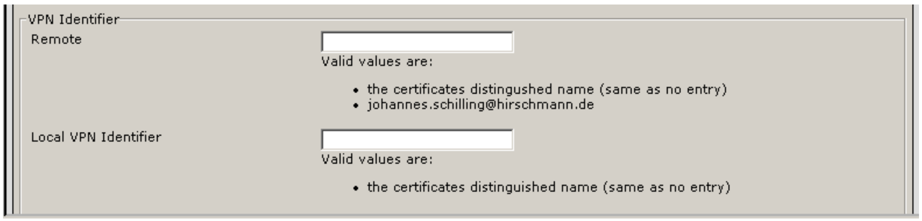
Pre-Shared Secret Key (PSK): complicated like 5Dx9qeD

This method is mainly used by older IPsec implementations. In this case both sides of the VPN authenticate each other with the same PSK.

To make the agreed upon key available to the mGuard, enter the agreed upon character string in the *Pre-Shared Secret Key (PSK)* entry field. To achieve security comparable to that of 3DES, the string should consist of about 30 characters selected at random and should include upper and lower case characters and digits.

☞ The *Pre-Shared Secret Key* cannot be used with dynamic (%any) IP addresses; fixed IP addresses or host names are required at both ends.

VPN Identifier



VPN Identifier

Remote

Valid values are:

- the certificates distingushed name (same as no entry)
- johannes.schilling@hirschmann.de

Local VPN Identifier

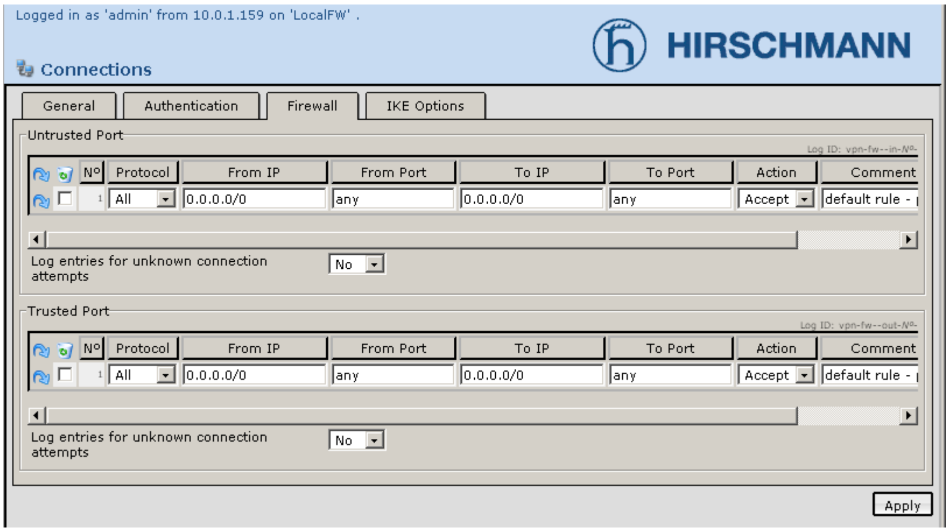
Valid values are:

- the certificates distinguished name (same as no entry)

Via the *VPN Identifier*, the VPN gateways can recognize which configurations belong to the same VPN connection.

If these fields are empty: In the case of X.509 certificates, the *Distinguished Name* of the certificate is utilized. In the case of PSK, the IP address of the VPN gateway is utilized.

Firewall



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Untrusted Port

Log ID: vpn-fw--in-Nº-

Nº	Protocol	From IP	From Port	To IP	To Port	Action	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule -

Log entries for unknown connection attempts: No

Trusted Port

Log ID: vpn-fw--out-Nº-

Nº	Protocol	From IP	From Port	To IP	To Port	Action	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule -

Log entries for unknown connection attempts: No

Firewall incoming (untrusted port), Firewall outgoing (trusted port)

While the settings made in the *Firewall* menu only affect non-VPN connections (see above under “Untrusted Port” on page 85), these settings affect just the VPN connection defined here. This means: If you have defined multiple VPN connections, you can restrict the outgoing or incoming access individually for each connection. You can have any attempts made to bypass these restrictions logged.

☒The VPN Firewall factory settings allow all connections via this VPN connection.
However, the settings for “Network Security → DoS” on page 94 do apply independently for each individual VPN connection.

☒If multiple firewall rules are set, they will be searched in the order in which they are listed from top to bottom until a suitable rule is found. This rule will then be applied. If further down in the list there are other rules which would also fit, they will be ignored.

☒In Single Client Transparent mode the firewall rules the real IP address is to be used for the client or left at 0.0.0.0/0, as only one client can be addressed through the tunnel.

As in the previous sections, you have the following options when making the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

From IP/To IP

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

From Port/To Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Transparent* mode, Reject has the same effect as Drop.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

Comment

An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

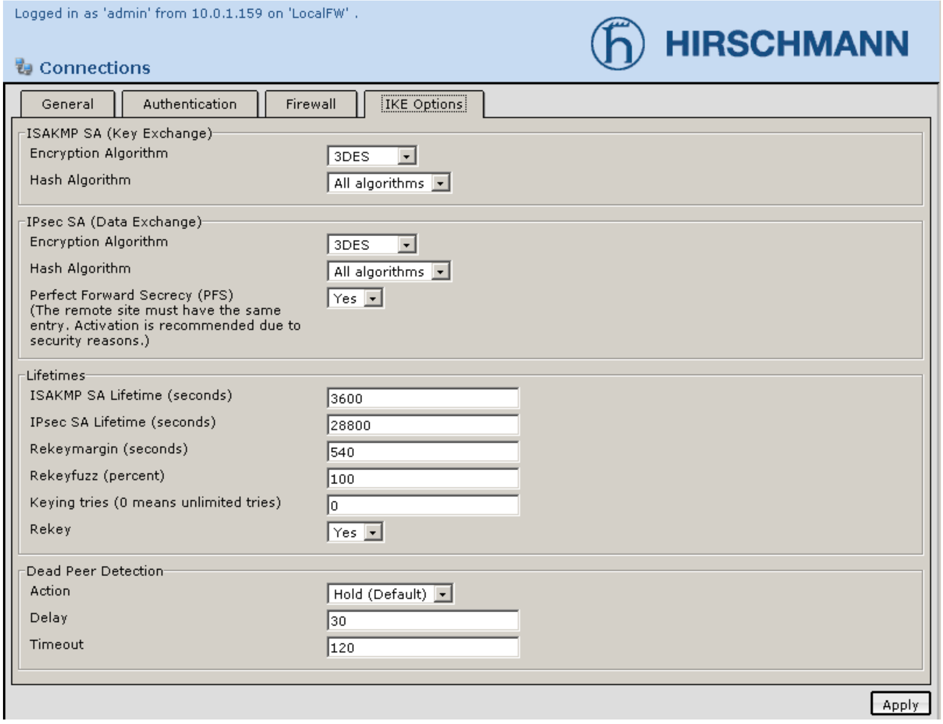
☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

IKE Options



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

ISAKMP SA (Key Exchange)

Encryption Algorithm	3DES
Hash Algorithm	All algorithms

IPsec SA (Data Exchange)

Encryption Algorithm	3DES
Hash Algorithm	All algorithms
Perfect Forward Secrecy (PFS) (The remote site must have the same entry. Activation is recommended due to security reasons.)	Yes

Lifetimes

ISAKMP SA Lifetime (seconds)	3600
IPsec SA Lifetime (seconds)	28800
Rekeymargin (seconds)	540
Rekeyfuzz (percent)	100
Keying tries (0 means unlimited tries)	0
Rekey	Yes

Dead Peer Detection

Action	Hold (Default)
Delay	30
Timeout	120

ISAKMP SA (Key Exchange)

Encryption algorithm

☞ Together with the administrator at the remote site, decide on which encryption technique should be used.

3DES-168 is the most commonly used algorithm and is therefore the default (factory) setting.

Basically the following applies: The greater the number of bits used by an encryption algorithm - specified by the appended number -, the more secure it is. The relatively new AES-256 protocol is therefore considered the most secure, but is not yet widely used.

The longer the key, the longer the time required by the encryption process. This latter point, however, is of no consequence for the mGuard, since it uses a hardware-based encryption technique. However, this aspect may be of significance for the remote site.

The algorithm designated as “Null” performs no encryption.

Hash Algorithm

Leave this setting on *All algorithms*. With this setting, it is does not matter whether the remote site uses MD5 or SHA-1.

IPsec SA (Data Exchange)

In contrast to *ISAKMP SA (Key Exchange)* (see above), this setting determines the method used for the exchange of data. This may be different from the Key Exchange but need not be.

Encryption Algorithm

See above

Hash Algorithm

See above

Perfect Forward Secrecy (PFS)

This method is used to increase the security of the data transfer. In IPsec, the key used for the data exchange is changed at certain intervals. In the case of PFS, a new random number is negotiated with the remote site instead of deriving it from a previously agreed on random number.

☞ Do not set this to **Yes**, unless the remote site also supports PFS.

☞ If you select the connection type *Transport (L2TP Microsoft Windows)*, set *Perfect Forward Secrecy (PFS)* to **No**.

Lifetimes

The keys of an IPsec connection will be renegotiated at certain intervals to increase the costs of an attack at the IPsec connection.

ISAKMP SA Lifetime

The lifetime of the ISAKMP SA keys in seconds.

The factory default is 3600 seconds (1 hour). The allowed maximum is 86400 seconds (24 hours).

IPsec SA Lifetime

The lifetime of the IPsec SA keys in seconds.

The factory default is 28800 seconds (8 hours). The allowed maximum is 86400 seconds (24 hours).

Rekeymargin

Minimal time interval before the old key expires during which a new key shall be negotiated. The factory default is 540 seconds (9 minutes).

Rekeyfuzz

Maximum in percent by which *Rekeymargin* shall be randomly increased.

This is to lower the load during key exchanges on machines with many VPN connections by serializing them. The factory default is 100 percent.

Keying tries

Number of attempts to negotiate new keys with the remote peer.

The special value 0 means unlimited attempts in case the connection is to be initiated by the mGuard, otherwise it means 5.

Rekey

When set to **Yes**, the mGuard will try to renegotiate keys when they expire.

Dead Peer Detection

When the remote peer supports the Dead Peer Detection (DPD) protocol, both peers can detect whether the connection is still valid or must be renegotiated. Without DPD, the connection must be either restarted manually or is unusable until the initiating sides SAs expire.

Action: Hold / Restart / Delete

The switch determines the action that is to be carried out when DPD has recognised a disruption in the IPsec connection.

In the case of **Hold** (default), an attempt to re-build the IPsec connection is made if it has been declared dead, but only when the locally connected network tries to send data to the receiver.

In the case of **Restart** the connection is re-built immediately.

In the case of **Clear** the connection will be deactivated until IPsec is restarted.

Delay

The length of time in seconds after which DPD Keep Alive queries will be sent to check the availability of the remote peer.

The factory default is 30 seconds.

Timeout

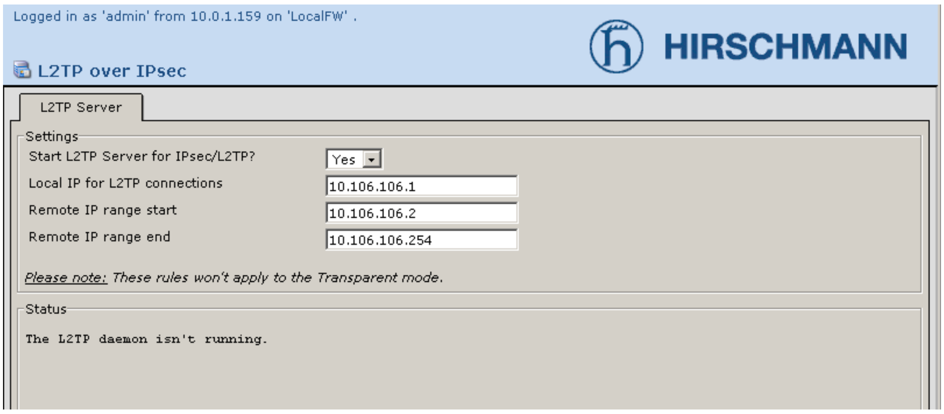
The length of time in seconds after which the remote peer will be declared dead if the Keep Alive queries are not answered.

The factory default is 120 seconds.

6.5.4 IPsec VPN → L2TP over IPsec

Together with VPN connections of connection type *transport*, the L2TP server allows remote peers to connection with IPsec/L2TP to the mGuard.

L2TP Server



Settings

Start L2TP Server for IPsec/L2TP?	Yes
Local IP for L2TP connections	10.106.106.1
Remote IP range start	10.106.106.2
Remote IP range end	10.106.106.254

Please note: These rules won't apply to the Transparent mode.

Status

```
The L2TP daemon isn't running.
```

Settings

Start L2TP Server for IPsec/L2TP? Yes / No
If you want to enable IPsec/L2TP connections, set this switch to **Yes**. It is then possible to establish incoming L2TP connections over IPsec, which dynamically assign IP addresses to the clients within the VPN.

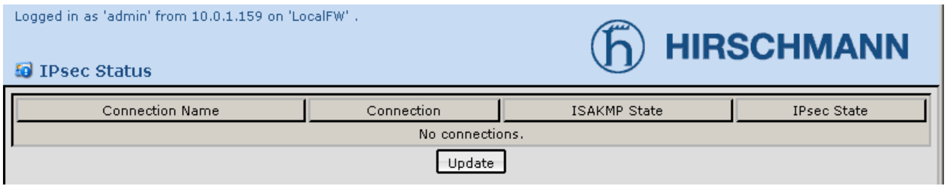
Local IP for L2TP connections
With the setting shown in the screenshot above, the mGuard will inform the remote site that the mGuard's address is 10.106.106.1.

Remote IPs for L2TP connections range
With the settings shown in the screenshot above, the mGuard will assigned IP addresses between 10.106.106.2 and 10.106.106.254 to the remote peers.

Status

Shows information about the L2TP status, when this type of connection has been selected. See "Connections" on page 99.
If this type of connection has not been selected, the screen shown above will be displayed.

6.5.5 IPsec VPN → IPsec Status


Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

IPsec Status

Connection Name	Connection	ISAKMP State	IPsec State
No connections.			

Shows the status of the IPsec connections.
The names of the VPN connections are listed on the left. On the right, you will find the current status of each connection.

GATEWAY
shows the IP addresses of the communicating VPN gateways

TRAFFIC
identifies the systems or networks which communicate via the VPN gateways.

ID
identifies the Distinguished Name (DN) of an X.509 certificate.

ISAKMP State
ISAKMP State (Internet security association and key management protocol) is given as "established", if the two VPN gateways involved have established a channel to exchange keys. In this case, they have been able to contact each other and all of the settings made on the configuration page up to and including "ISAKMP SA" were correct.

IPsec State
IPsec State is given as "established", if IPsec encryption is activated when communicating. In this case, the entries made under "IPsec SA" and "Tunnel Settings" were also correct.

In the event of problems, we recommend that you examine the VPN logs of the system to which the connection was setup. The basis for this recommendation is that for reasons of security exhaustive error messages are not returned to the initiating system.

If the display shows:
ISAKMP SA established, IPsec State: WAITING
This indicates that:
the authentication was successful, but the other parameters are not correct: Do the connection types (Tunnel, Transport) match? If Tunnel has been selected, do the network address areas match at both ends?

If the display shows:
IPsec State: IPsec SA established
This indicates that:
the VPN connection has been successfully setup and can be used. If this is not the case, there must be a problem with the remote VPN gateway. In this case, disable and enable the connection to re-establish the connection.

6.6 Menu AntiVirus (not on control unit)

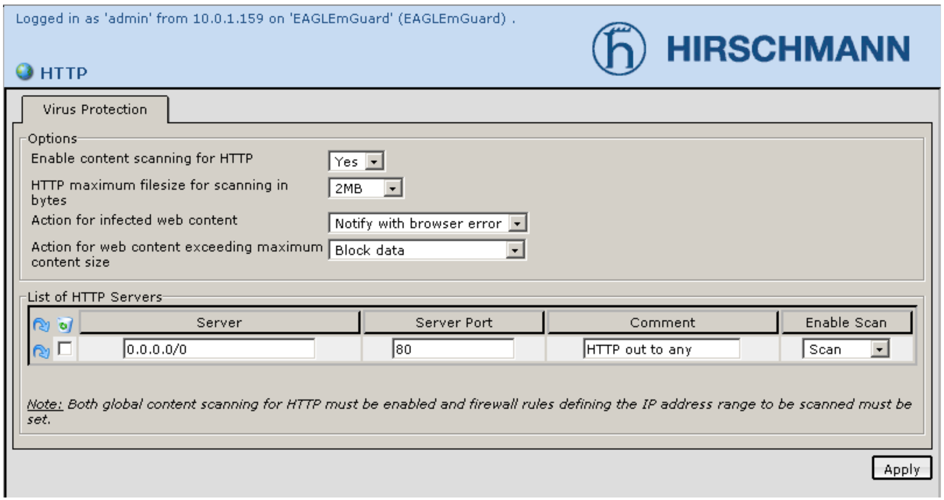
6.6.1 AntiVirus → HTTP

Requirements:

The following requirements must be fulfilled for the use of the virus filter:

- Anti-virus license has been installed. Instructions on how to request and install a license can be found under the section “Basic Settings → Update” on page 71.
- Access to an update server with the current versions of the virus signatures (see section “Basic Settings → Update” on page 71).

Virus Protection



Logged in as 'admin' from 10.0.1.159 on 'EAGLEmGuard' (EAGLEmGuard) .

HTTP

Virus Protection

Options

Enable content scanning for HTTP	Yes
HTTP maximum filesize for scanning in bytes	2MB
Action for infected web content	Notify with browser error
Action for web content exceeding maximum content size	Block data

List of HTTP Servers

	Server	Server Port	Comment	Enable Scan
☐	0.0.0.0/0	80	HTTP out to any	Scan

Note: Both global content scanning for HTTP must be enabled and firewall rules defining the IP address range to be scanned must be set.

The HTTP protocol is not only used by web browsers to retrieve data from web sites, but is also used in many other applications. It is also used, for example, to download files, e.g. software updates, or to initialize multimedia streams.

- The transferred file will only passed on after it has been loaded completely and checked. Consequently, user software may react less quickly when downloading larger files or whenever the download speeds are slow.
- To check the anti-virus protection for HTTP, you can download the safe Eicar test virus which is available for test purposes at http://www.eicar.org/anti_virus_test_file.htm.

Options

Anti-virus protection for HTTP: Yes / No

In the case of **Yes**, files received are scanned for viruses by mGuard if they arrive via HTTP connections contained in the list of HTTP servers below.

Scanning up to a pre-set volume of:

5 MB. The maximum size of the files to be checked is specified here. Files that are larger are not scanned. Depending on the “When size limit is exceeded” setting, an error message is sent to the browser in the event of a file exceeding the size limit, or the system automatically switches to throughput mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's client software (browser or download manager) and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to download the file
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the data pass unscanned”.

Action for infected web content

Notify with browser error

If the virus filter detects a virus in the data transferred from an HTTP server to the HTTP client, an error message will be sent to the HTTP client. The handling of this error message depends on the respective HTTP client. A web browser will display the error message in the form of an HTML page. If a file that is downloaded within an HTML page - e.g. a graphic file - is infected, this file will not be displayed in the browser. If a download manager is used to download a file via HTTP, the error message will be displayed by the download manager.

Action for web content exceeding the maximum content size

Let data pass unscanned

When this option is selected the virus filter will allow the files, which exceed the filesize set, to pass through unscanned.

☞ In this case, the data is not checked for viruses!

Block data

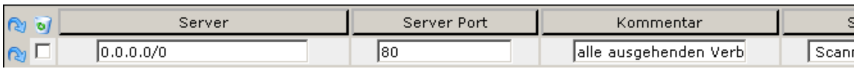
If this option is selected, the system will terminate the download and send an error message to the client software whenever the content exceeds the maximum size.

List of HTTP Servers

You can select the servers, whose traffic should be filtered, and specify for each IP address whether or not the anti-virus protection should be activated. It is also possible to enter “trusted” servers.

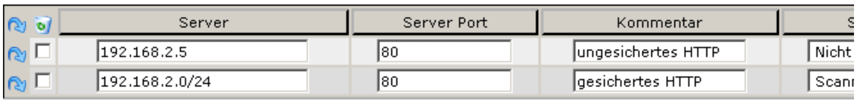
Examples:

Global activation of the anti-virus protection for HTTP:



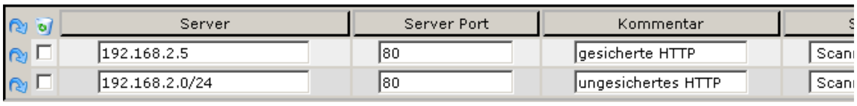
	Server	Server Port	Kommentar	S
☐	0.0.0.0/0	80	alle ausgehenden Verb	Scan

Scan a subnet and exclude a “trusted” HTTP server:



	Server	Server Port	Kommentar	S
☐	192.168.2.5	80	ungesichertes HTTP	Nicht
☐	192.168.2.0/24	80	gesichertes HTTP	Scan

Scan a single “untrusted” SMTP server in a subnet:



	Server	Server Port	Kommentar	S
☐	192.168.2.5	80	gesicherte HTTP	Scan
☐	192.168.2.0/24	80	ungesichertes HTTP	Scan

☒ To activate the virus filter for HTTP or “FTP over HTTP” connections over a proxy, insert a new row and change the default port 80 to the proxy’s port. Common proxy ports are 3128 and 8080.

☒ The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.

☒ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.

☒ Scanning for viruses may allow outgoing connections which are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 89 to adjust this behaviour.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic of all HTTP servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

⌦ Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the HTTP protocol in this field. The default setting for the HTTP port is **80**.

Comment

An informational comment for this rule.

Scan

Scan

The virus filter is activated for the server specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

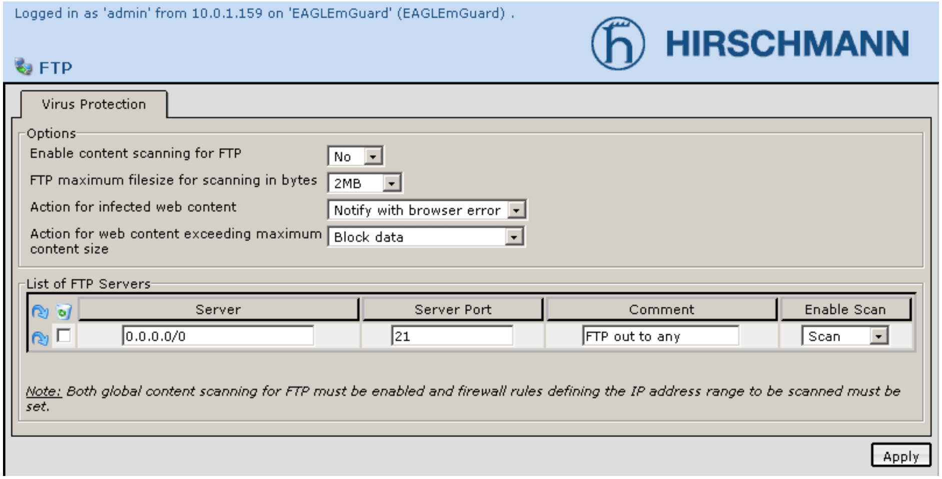
6.6.2 Web Security → FTP

Requirements:

The following requirements must be fulfilled for the use of the virus filter:

- Anti-virus license has been installed. Instructions on how to request and install a license can be found under the section “Basic Settings → Update” on page 71.
- Access to an update server with the current versions of the virus signatures (see section “Basic Settings → Update” on page 71).

Virus Protection



Logged in as 'admin' from 10.0.1.159 on 'EAGLEmGuard' (EAGLEmGuard) .

Options

Enable content scanning for FTP: No

FTP maximum filesize for scanning in bytes: 2MB

Action for infected web content: Notify with browser error

Action for web content exceeding maximum content size: Block data

List of FTP Servers

	Server	Server Port	Comment	Enable Scan
□	0.0.0.0/0	21	FTP out to any	Scan

Note: Both global content scanning for FTP must be enabled and firewall rules defining the IP address range to be scanned must be set.

The FTP protocol is used for up- and download of files.

- The transferred file will only passed on after it has been loaded completely and checked. Consequently, user software may react less quickly when downloading larger files or whenever the download speeds are slow.

- To check the anti-virus protection for FTP, you can download the safe Eicar test virus which is available for test purposes at http://www.eicar.org/anti_virus_test_file.htm.
- The mGuard can only be used to secure the FTP-client.

Options

Anti-virus protection for FTP: Yes / No

In the case of **Yes**, files received are scanned for viruses by mGuard if they arrive via FTP connections contained in the list of FTP servers below.

Scanning up to a pre-set volume of:

5 MB. The maximum size of the files to be checked is specified here. Files that are larger are not scanned. Depending on the “When size limit is exceeded” setting, an error message is sent to the client in the event of a file exceeding the size limit, or the system automatically switches to throughput mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's client software and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to download/upload the file
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the data pass unscanned”.

Action for infected content

Notify with browser error

If the virus filter detects a virus in the data transferred between the FTP server and the FTP client, an error message will be sent to the FTP client. The handling of this error message depends on the respective FTP client.

Action for web content exceeding the maximum content size

Let data pass unscanned

When this option is selected the virus filter will allow the files, which exceed the filesize set, to pass through unscanned.

⌦ In this case, the data is not checked for viruses!

Block data

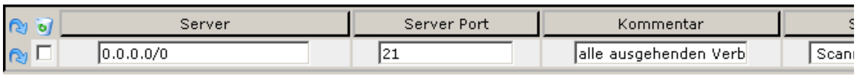
If this option is selected, the system will terminate the download and send an error message to the client software whenever the content exceeds the maximum size.

List of FTP Servers

You can select the servers, whose traffic should be filtered, and specify for each IP address whether or not the anti-virus protection should be activated. It is also possible to enter “trusted” servers.

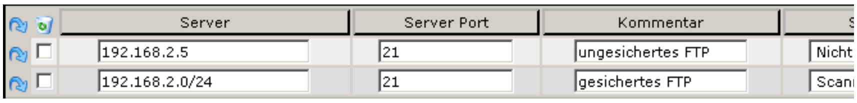
Examples:

Global activation of the anti-virus protection for FTP:



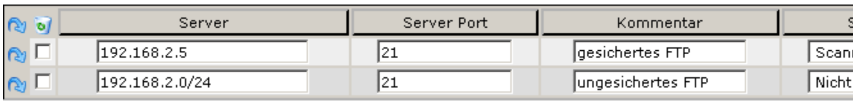
	Server	Server Port	Kommentar	S
□	0.0.0.0/0	21	alle ausgehenden Verb	Scan

Scan a subnet and exclude a “trusted” FTP server:



		Server	Server Port	Kommentar	S
	☐	192.168.2.5	21	ungesichertes FTP	Nicht
	☐	192.168.2.0/24	21	gesichertes FTP	Scan

Scan a single “untrusted” FTP server in a subnet:



		Server	Server Port	Kommentar	S
	☐	192.168.2.5	21	gesichertes FTP	Scan
	☐	192.168.2.0/24	21	ungesichertes FTP	Nicht

⌧ To activate the virus filter for FTP connections over a proxy, insert a new row and change the default port 21 to the proxy’s port.

⌧ The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.

⌧ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.

⌧ Scanning for viruses may allow outgoing connections which are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 89 to adjust this behaviour.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic of all FTP servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

⌧ Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the FTP protocol in this field. The default setting for the FTP port is **21**.

Comment

An informational comment for this rule.

Scan

Scan

The virus filter is activated for the server specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

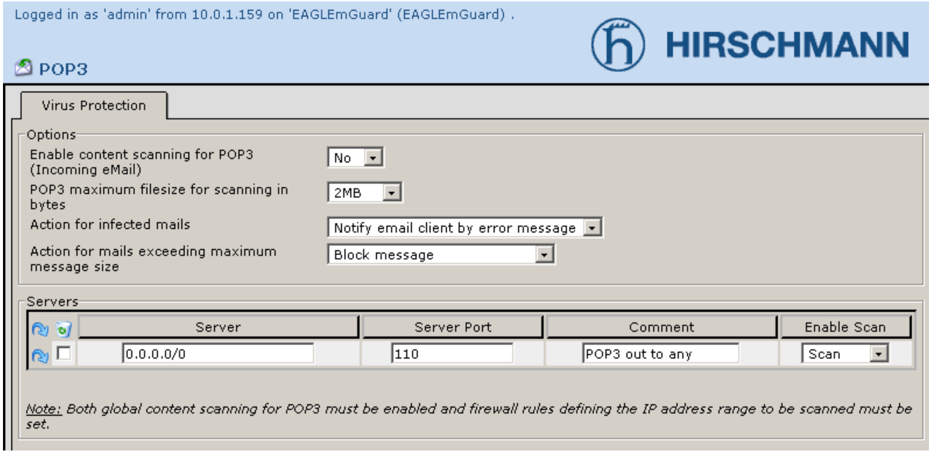
6.6.3 AntiVirus → POP3

Requirements:

The following requirements must be fulfilled for the use of the virus filter:

- Anti-virus license has been installed. Instructions on how to request and install a license can be found under the section “Basic Settings → Update” on page 71.
- Access to an update server with the current versions of the virus signatures (see section “Basic Settings → Update” on page 71).

Virus Protection



Logged in as 'admin' from 10.0.1.159 on 'EAGLEmGuard' (EAGLEmGuard) .

POP3

Virus Protection

Options

Enable content scanning for POP3 (Incoming eMail)	No
POP3 maximum filesize for scanning in bytes	2MB
Action for infected mails	Notify email client by error message
Action for mails exceeding maximum message size	Block message

Servers

Server	Server Port	Comment	Enable Scan
0.0.0.0/0	110	POP3 out to any	Scan

Note: Both global content scanning for POP3 must be enabled and firewall rules defining the IP address range to be scanned must be set.

Your e-mail client uses the POP3 protocol for incoming e-mail.

☞ The virus filter can only check unencrypted data for viruses. Consequently, you should not activate encryption options such as STLS or SSL. Encrypted authentication using AUTH is, however, usable, since the e-mail itself is not encrypted.

Options

Anti-virus protection for POP3 (E-mail pickup): Yes / No

In the case of **Yes**, files received are scanned for viruses by mGuard if they arrive via POP3 connections contained in the list of POP3 servers below.

☞ Tip: When using a POP3 connection, most e-mail clients will pick up all of the e-mails during a single connection. In this case, the new settings will first take effect after the last e-mail is collected from the server during the current connection. Consequently, to change the settings when an e-mail transfer is in process, first cancel the transfer.

POP3 maximum filesize for scanning in bytes

With this parameter, you can set the maximum size of the files to be checked. If this limit is exceeded, the system will - depending on the setting “Action for mails exceeding the maximum message size” - block the e-mail and send an error message back to the e-mail client or it will automatically switch to “Let the message pass unscanned” mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's e-mail client and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to download the file
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the message pass unscanned”.

Please note that - depending on the coding scheme used - the size of the attachment may be larger than the original file.

Action for infected mails

Notify recipient by e-mail:

If the virus filter detects a virus, the recipient will be informed by e-mail.

Notify e-mail client by error message:

If the virus filter detects a virus, the recipient will be informed by an error message sent to the e-mail client.

☞ If the parameter “Delete received messages from server” has been set in the e-mail client software and the “Action for infected mails” has been set to “Notify recipient by e-mail”, the infected e-mail will be deleted on the server, since the e-mail client will assume that the e-mail has been successfully transferred. If you do not wish to have the infected mail deleted (e.g. if you wish to download the infected e-mail in some other manner), only use the option “Notify e-mail client by error message”.

Action for mails exceeding the maximum message size

Let the message pass unscanned

When this option is selected the virus filter will allow the messages, which exceed the filesize set, to pass through unscanned.

☞ In this case, the mail will not be checked for viruses!

Block message

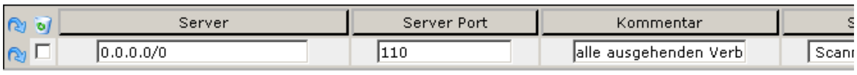
When this option is selected, an error code will be returned to the e-mail client and the e-mail will be blocked.

List of POP3 servers

Indicate which servers’ files should be scanned for viruses. By enabling or disabling the anti-virus function beside each individual entry or server, respectively, you can, for example, set an exception rule for a subsequent comprehensive rule. This allows you to define “trusted” servers – see the example illustrated below.

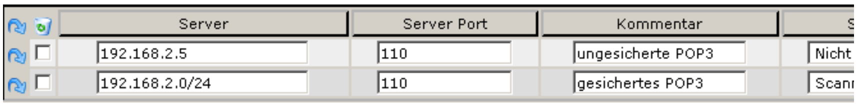
Examples:

Global activation of the anti-virus protection for POP3:



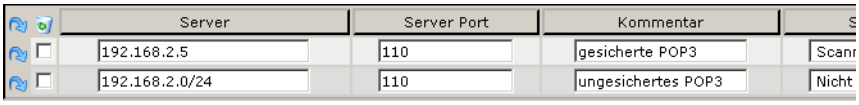
	Server	Server Port	Kommentar	S
□	0.0.0.0/0	110	alle ausgehenden Verb	Scanı

Scan a subnet and exclude a “trusted” POP3 server:



	Server	Server Port	Kommentar	S
□	192.168.2.5	110	ungesicherte POP3	Nicht
□	192.168.2.0/24	110	gesichertes POP3	Scanı

Scan a single “untrusted” POP3 server in a subnet:



	Server	Server Port	Kommentar	S
□	192.168.2.5	110	gesicherte POP3	Scanı
□	192.168.2.0/24	110	ungesichertes POP3	Nicht

⌧ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.

⌦The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.

⌦Scanning for viruses may allow outgoing connections which are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 89 to adjust this behaviour.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic of all POP3 servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

⌦Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the POP3 protocol in this field. The default setting for the POP3 port is **110**.

Comment

An informational comment for this rule.

Scan

Scan

The virus filter is activated for the servers specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

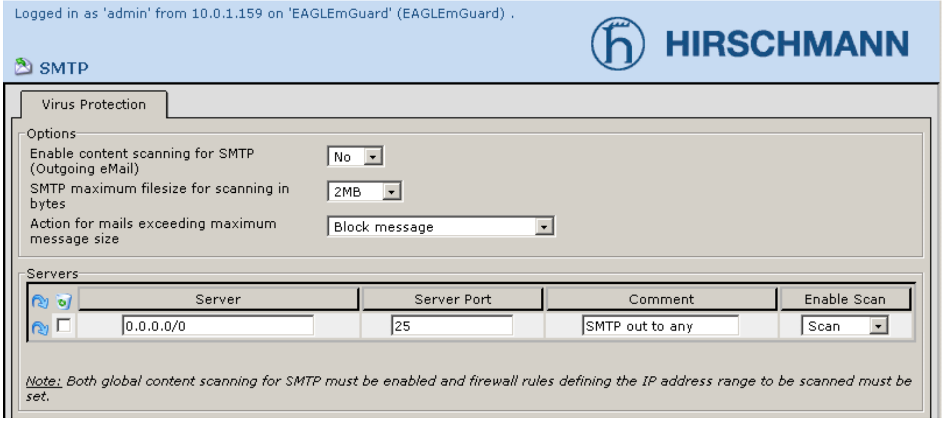
6.6.4 AntiVirus → SMTP

Requirements:

The following requirements must be fulfilled for the use of the virus filter:

- Anti-virus license has been installed. Instructions on how to request and install a license can be found under the section "Basic Settings → Update" on page 71.
- Access to an update server with the current versions of the virus signatures (see section "Basic Settings → Update" on page 71).

Virus Protection



Logged in as 'admin' from 10.0.1.159 on 'EAGLEmGuard' (EAGLEmGuard) .

Options

Enable content scanning for SMTP (Outgoing eMail): No

SMTP maximum filesize for scanning in bytes: 2MB

Action for mails exceeding maximum message size: Block message

Servers

	Server	Server Port	Comment	Enable Scan
□	0.0.0.0/0	25	SMTP out to any	Scan

Note: Both global content scanning for SMTP must be enabled and firewall rules defining the IP address range to be scanned must be set.

The SMTP protocol is used by e-mail clients or mail transfer agents (MTA) to send e-mails.

☞ The virus filter can only check unencrypted data for viruses.

Consequently, you should not activate encryption options such as TLS. If a virus is detected or an error occurs, an e-mail with an error code will be sent to the sender and an entry will be made in the anti-virus log. The intended recipient will receive neither the infected mail nor a message.

Options

Anti-virus protection for SMTP (E-mail transmission): Yes / No

In the case of Yes, files to be sent are scanned for viruses by mGuard if they are to be transmitted via SMTP connections that are specified in the list of SMTP servers below.

Scanning up to a pre-set volume of

5 MB. The maximum size of the files to be checked is specified here. Files that are larger are not scanned. Depending on the "When size limit is exceeded" setting, an error message is sent to the SMTP client and the e-mail is not delivered in the event of a file exceeding the size limit, or the system automatically switches to throughput mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's e-mail client and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to send the message.
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to "Let the message pass unscanned".

Please note that - depending on the coding scheme used - the size of the attachment may be larger than the original file.

Action for mails exceeding the maximum message size

Let the message pass unscanned

When this option is selected the virus filter will allow the messages, which exceed the filesize set, to pass through unscanned.

☞ In this case, the message is not checked for viruses!

Block message

When this option is selected, an error code will be returned to the e-mail client and the e-mail will be blocked.

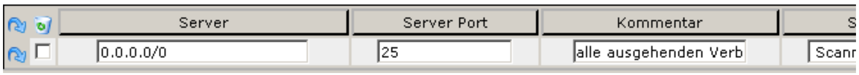
List of SMTP servers

Indicate which server connections should be scanned for viruses.

By enabling or disabling the anti-virus function beside each individual entry or server, respectively, you can, for example, set an exception rule for a subsequent comprehensive rule. This allows you to define “trusted” servers – see the example illustrated below

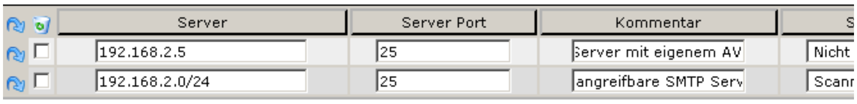
Examples:

Global activation of the anti-virus protection for SMTP:



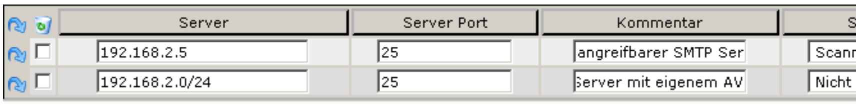
	Server	Server Port	Kommentar	S
☐	0.0.0.0/0	25	alle ausgehenden Verb	Scann

Scan a subnet and exclude a SMTP server:



	Server	Server Port	Kommentar	S
☐	192.168.2.5	25	Server mit eigenem AV	Nicht
☐	192.168.2.0/24	25	angreifbare SMTP Serv	Scann

Scan traffic to a single SMTP server in a subnet:



	Server	Server Port	Kommentar	S
☐	192.168.2.5	25	angreifbarer SMTP Ser	Scann
☐	192.168.2.0/24	25	Server mit eigenem AV	Nicht

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 44.

⌦ The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.

⌦ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.

⌦ Scanning for viruses may allow outgoing connections which are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 89 to adjust this behaviour.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic to all SMTP servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 140.

⌦ Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the SMTP protocol in this field. The default setting for the SMTP port is **25**.

Comment

An informational comment for this rule.

Scan

Scan

The virus filter is activated for the server specified in this rule.

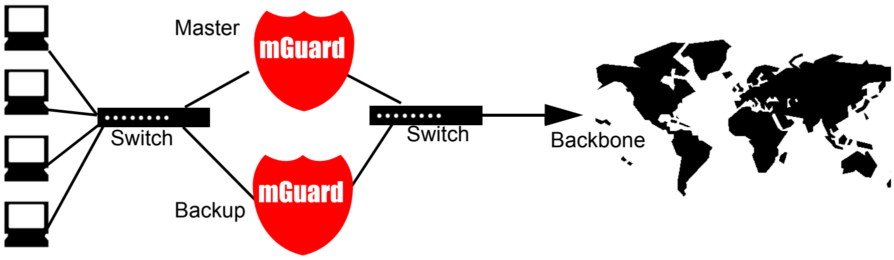
No Scan

The virus filter is deactivated for the server specified in this rule.

6.7 Menu redundancy

6.7.1 *Firewall Redundancy*

It is possible to combine two mGuards to a single virtual router with the help of the redundancy ability.



In so doing, the second mGuard (backup) takes over the function of the first mGuard (master) in the event of an error.

The redundancy feature allows two mGuards to be configured to operate as a virtual router. In case of an error, one mGuard (the *backup*) will take over the functionality of the other mGuard (previously working as the *master*).

Additionally, the state of the statefull firewall is synchronized between both mGuards so that, in case of a takeover, current connections will not be interrupted.

⌧ Prerequisite: Both mGuards must be configured accordingly. The firewall configuration should be identical to avoid problems after a switch.

⌧ Redundancy can only be used in router mode, static Transparent mode with management IP or multi Transparent mode.

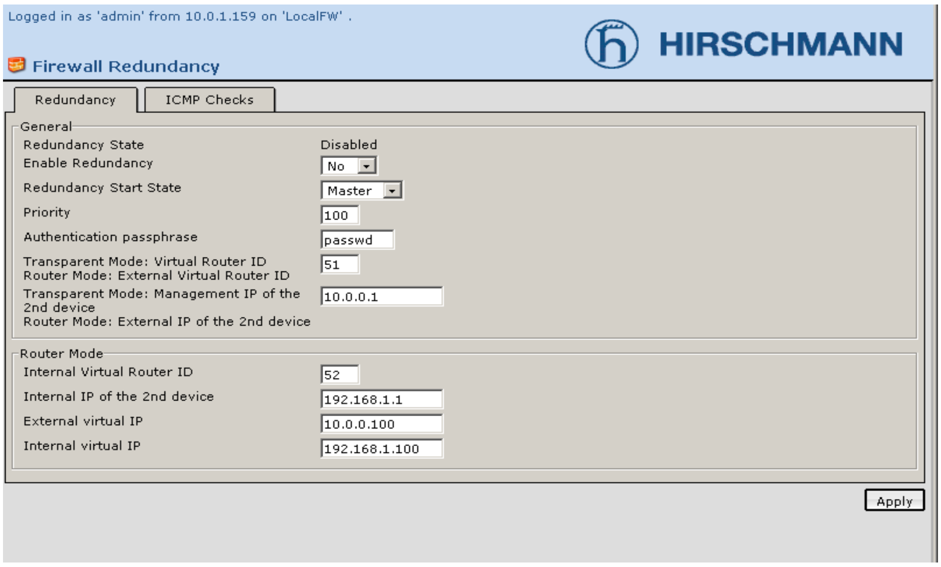
⌧ The mGuards operating as virtual router must not be used as a VPN gateway.

⌧ Devices connected to the internal network of the virtual router configuration must be configured to use the internal virtual IP as the default gateway.

The following features are supported by the virtual router configuration:

- Incoming/Outgoing firewall rules
- NAT (IP-Masquerading, i.e. traffic is NATed to the external virtual IP)
- 1to1 NAT
- Port forwarding (use the external virtual IP as *Incoming on IP*)
- MAC-Filter

Redundancy



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Firewall Redundancy

General

Redundancy State	Disabled
Enable Redundancy	No
Redundancy Start State	Master
Priority	100
Authentication passphrase	passwd
Transparent Mode: Virtual Router ID Router Mode: External Virtual Router ID	51
Transparent Mode: Management IP of the 2nd device Router Mode: External IP of the 2nd device	10.0.0.1

Router Mode

Internal Virtual Router ID	52
Internal IP of the 2nd device	192.168.1.1
External virtual IP	10.0.0.100
Internal virtual IP	192.168.1.100

General

Redundancy State

Shows the current redundancy state of this mGuard.

Enable Redundancy

Enable/Disable the redundancy feature.

Redundancy Start State

The state of this mGuard during activation of redundancy (master or backup).

Priority

Defines which mGuard will operate as the master.

In case the priorities are different, the mGuard with the higher priority will operate as the master as long as it does not fail.

If both mGuards have the same priority and the backup becomes the master in case of a failure, it will continue to work as the master even when the other mGuard becomes available again.

Values between 1 and 254 are possible.

Authentication passphrase

This password is to protect against misconfiguration among different virtual routers.

The password must be the same on both mGuards. It will be transmitted in clear text and should not be identical with other security relevant passwords.

Transparent Mode: Virtual Router ID
Routermode: External Virtual Router ID

An ID between 1 and 255 which must be the same on both mGuards and identifies the virtual router.

Transparent Mode: Management IP of the 2nd device
Routermode: External IP of the 2nd device

In Transparent mode the management IP of the other mGuard, in router mode the external IP of the other mGuard.

Router Mode

The following values need to be set if the mGuards are operated in router mode.

Internal Virtual Router ID

An ID between 1 and 255 which must be the same on both mGuards and identifies the virtual router on the internal interface.

Internal IP of the 2nd device

The internal IP of the other mGuard.

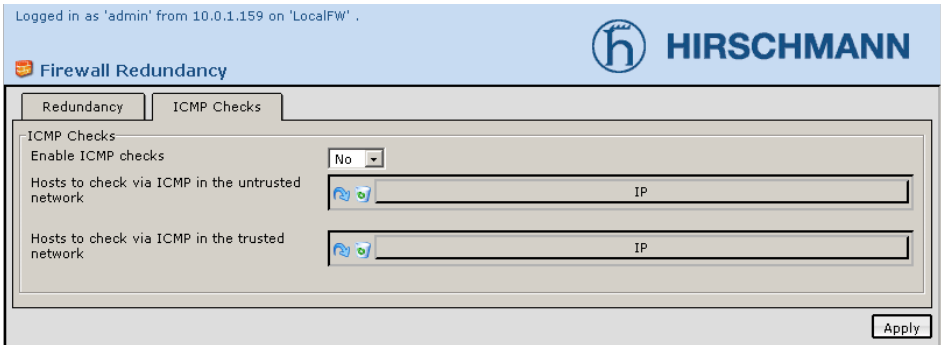
External virtual IP

IP of the virtual router on the external interface (WAN).

Internal virtual IP

IP of the virtual router on the internal interface (LAN). Clients inside the internal network should use this IP as their default gateway.

ICMP Checks



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Firewall Redundancy

ICMP Checks

Enable ICMP checks: No

Hosts to check via ICMP in the untrusted network: IP

Hosts to check via ICMP in the trusted network: IP

ICMP checks provide an additional way to monitor the network connections between mGuards working as a virtual router.

If one of the two direct Ethernet connections that exist between the LAN ports of the two mGuards (to the left of the two mGuards in the illustration on page 139) and between their WAN ports (to the right of the two mGuards in the illustration) fails, the backup becomes the master. The Virtual Router Redundancy Protocol (VRRP) utilised by the Guard can’t, however, inform master of this while it is still operating.

With ICMP checks (ICMP ping), the master can check its connections to the backup and deactivate itself in case its internal (trusted) or external (untrusted) connections to the backup failed.

Enable ICMP Checks

The master mGuard will check the connection to the backup mGuard using the ICMP ping protocol.

In case the backup mGuard can not be reached, the *Hosts to check via ICMP in the external/internal network* will be tried. If these checks fail as well, the master mGuard will deactivate itself.

Hosts to check via ICMP in the external (untrusted) network

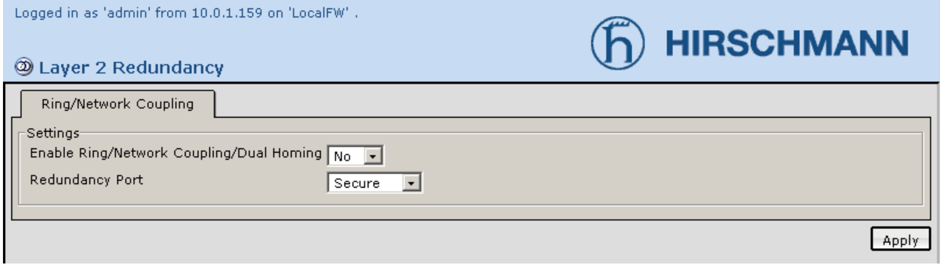
Hosts in the external network to be checked. The hosts have to be able to answer to the ICMP echo requests.

Hosts to check via ICMP in the internal (trusted) network

Hosts in the internal network to be checked.The hosts have to be able to answer to the ICMP echo requests.

6.7.2 Layer 2 Redundancy

Ring / Network Coupling



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Settings

Enable Ring/Network Coupling/Dual Homing: No

Redundancy Port: Secure

Settings

Enable Ring/Network Coupling/Dual Homing: Yes / No
When activated, the link status of one ethernet port will be transfered to the other ethernet port whereby interruptions in the network can be traced more easily.

Redundancy Port: Internal (trusted) / External (untrusted)
Internal: In case the connection on the LAN port goes down/up, the WAN port will be set down/up also.
External: In case the connection on the WAN port goes down/up, the LAN port will be set down/up also.

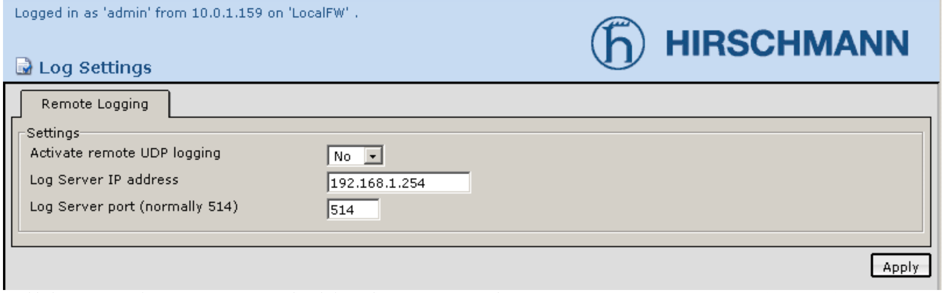
6.8 Menü Diagnosis

The term ‘logging’ is understood to mean the recording of event messages, e.g., about settings that have been set, about firewall rules taking effect, about errors, etc.

Log entries are recorded in different categories and can also be displayed according to categories – see “Diagnosis → Event logs” on page 127

6.8.1 Log → Settings

Remote Logging



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Log Settings

Remote Logging

Settings

Activate remote UDP logging: No

Log Server IP address: 192.168.1.254

Log Server port (normally 514): 514

All log entries are recorded in the mGuard's temporary memory (RAM). Once the space for log entries has been filled, the oldest log entries will be overwritten. Furthermore, if the mGuard is switched off, all log entries are deleted.

If you wish to keep a copy of the log, the log entries can be sent to an external system. This is particularly useful if you wish to have centralized administration of the logs.

Settings

Activate remote UDP logging Yes / No

If all log entries should be sent to an external (specified below) log server, set this option to **Yes**.

Log Server IP address

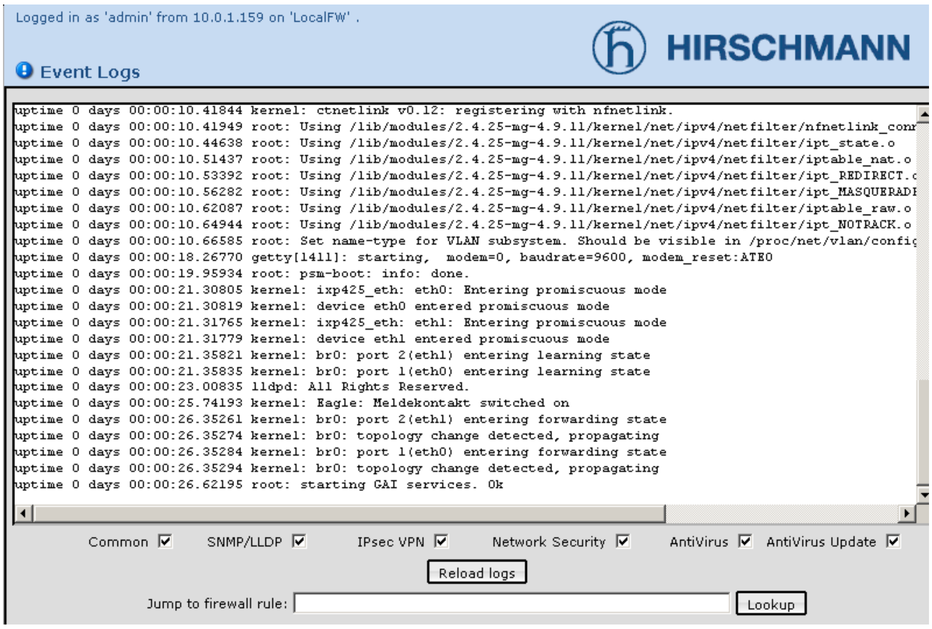
Enter the IP address of the log server to which the log entries should be sent via UDP.

☞ This entry must be an IP address - not a hostname! This function does not support hostnames, since, if it did, it would not be possible to log the loss of a DNS server.

Log Server port

Enter the port of the log server to which the log entries should be sent via UDP. Standard: 514

6.8.2 Diagnosis → Event logs



```
uptime 0 days 00:00:10.41844 kernel: ctnetlink v0.12: registering with nfnetlink.
uptime 0 days 00:00:10.41949 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/nfnetlink_conr
uptime 0 days 00:00:10.44638 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/ipt_state.o
uptime 0 days 00:00:10.51437 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/iptable_nat.o
uptime 0 days 00:00:10.53392 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/ipt_REDIRECT.c
uptime 0 days 00:00:10.56282 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/ipt_MASQUERADE
uptime 0 days 00:00:10.62087 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/iptable_raw.o
uptime 0 days 00:00:10.64944 root: Using /lib/modules/2.4.25-mg-4.9.11/kernel/net/ipv4/netfilter/ipt_NOTRACK.o
uptime 0 days 00:00:10.66585 root: Set name-type for VLAN subsystem. Should be visible in /proc/net/vlan/config
uptime 0 days 00:00:18.26770 getty[1411]: starting,  modem=0, baudrate=9600, modem_reset:ATE0
uptime 0 days 00:00:19.95934 root: psm-boot: info: done.
uptime 0 days 00:00:21.30805 kernel: ixp425_eth: eth0: Entering promiscuous mode
uptime 0 days 00:00:21.30819 kernel: device eth0 entered promiscuous mode
uptime 0 days 00:00:21.31765 kernel: ixp425_eth: eth1: Entering promiscuous mode
uptime 0 days 00:00:21.31779 kernel: device eth1 entered promiscuous mode
uptime 0 days 00:00:21.35821 kernel: br0: port 2(eth1) entering learning state
uptime 0 days 00:00:21.35835 kernel: br0: port 1(eth0) entering learning state
uptime 0 days 00:00:23.00835 lldpd: All Rights Reserved.
uptime 0 days 00:00:25.74193 kernel: Eagle: Meldekontakt switched on
uptime 0 days 00:00:26.35261 kernel: br0: port 2(eth1) entering forwarding state
uptime 0 days 00:00:26.35274 kernel: br0: topology change detected, propagating
uptime 0 days 00:00:26.35284 kernel: br0: port 1(eth0) entering forwarding state
uptime 0 days 00:00:26.35294 kernel: br0: topology change detected, propagating
uptime 0 days 00:00:26.62195 root: starting GAI services. Ok
```

Common ☑ SNMP/LLDP ☑ IPsec VPN ☑ Network Security ☑ AntiVirus ☑ AntiVirus Update ☑

Reload logs

Jump to firewall rule: Lookup

Depending on which mGuard functions were active, the corresponding checkboxes for filtering entries according to category are displayed below the log entries. Enable the checkbox(es) for the desired category(ies) and click the **Reload logs** button to display one or more categories

Common

All log entries which are not related to the other categories appear here.

Network Security

When logging of firewall events was choosen during the definition of firewall rules (Log = yes), then these logged events are show here.

Log ID and number for tracing errors

Log entries that refer to the firewall rules listed below have a log ID and a number. Using the log ID and number, it is possible to trace the firewall rule that the corresponding log entry refers to and that led to the event in question.

Firewall rules and their log ID

- Packet filters:
  Network security → Packet filters → Incoming rules / Outgoing rules menu **Log ID: fw-incoming** or **fw-outgoing, respectively**
- Firewall rules for VPN connections:
  `IPsec VPN → Connections → Firewall incoming / outgoing menu`
  `Log ID:` **`vpn-fw-in`** `or` **`vpn-fw-out`**`, respectively`
- Firewall rules for web access through mGuard via HTTPS: Administration Security Web → Access → Access → menu
  Log ID: **`fw-https-access`**
- Firewall rules for web access through mGuard via SNMP: Security → SNMP → Query menu
  Log ID: **`fw-snmp-access`**
- Firewall rules for SSH remote access to the mGuard:
  Basic Settings → System → Shell access menu
  Log ID: **`fw-ssh-access`**
- Firewall rules for the user firewall:

Network security → User firewall → Firewall rules menu
Log ID: **`ufw-`**

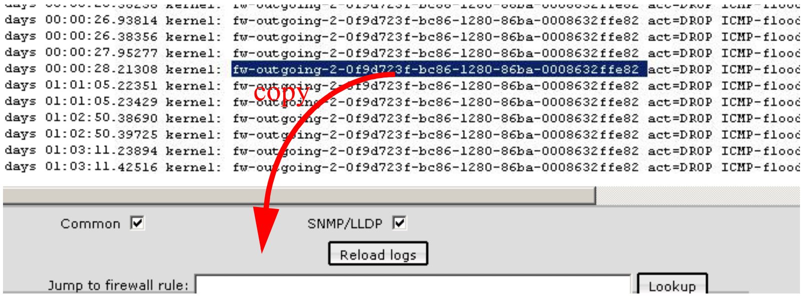
- Rules for NAT, port forwarding
  Network security → NAT → Port forwarding menu
  Log ID: **`fw-portforwarding`**

Searching for firewall rules on the basis of a network security log

If the **Network security** checkbox is enabled, the **Jump to firewall rule** search field is displayed below the Get the logs button so that the relevant log entries can be displayed.

Proceed as follows if you want to trace the firewall rule that a log entry in the *network security* category references and that resulted in the relevant event:

1. Mark the section that contains the log ID and number in the relevant log entry, for example: fw-https-access-1-2e49ed19-e930-161b-922-00cbe010f52



```
days 00:00:26.93814 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 00:00:26.38356 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 00:00:27.95277 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 00:00:28.21308 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 01:01:05.22351 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 01:01:05.23429 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 01:02:50.38690 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 01:02:50.39725 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 01:03:11.23894 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
days 01:03:11.42516 kernel: fw-outgoing-2-0f9d723f-bc86-1280-86ba-0008632ffe82 act=DROP ICMP-flood
```

Common ☑ SNMP/LLDP ☑

Jump to firewall rule:

2. Copy this section into the **Jump to firewall rule** field via the clipboard.
3. Click the Search button.

   Result:

   The configuration page containing the firewall rule that the log entry refers to is displayed.

Blade

In addition to the error messages, the following messages are output on the blade controller:

(The areas enclosed by < and > are replaced by the respective data in the log entries.)

General messages:

```
blade daemon "<version>" starting ...
Blade[<bladenr>] online
Blade[<bladenr>] is mute
Blade[<bladenr>] not running
Reading timestamp from blade[<bladenr>]
```

When activating a configuration profile on a blade:

```
Push configuration to blade[<bladenr>]
reconfiguration of blade[<bladenr>] returned <returncode>
blade[<bladenr>] # <text>
```

When retrieving a configuration profile from blade:

```
Pull configuration from blade[<bladenr>]
Pull configuration from blade[<bladenr>] returned <returncode>
```

AntiVirus

The Anti-Virus Log contains the following messages from the virus filter:

- The names of any viruses found together with the following information: name of the file and (in the case of an e-mail) the sender, date and subject.

- Warnings sent whenever the system has passed a file through unscanned because it was larger than the maximum file size.
- Startup and shutdown of the virus filter programs.
- Error messages from the scan-Engine and the virus filter.

Error Messages

Virus Detection
A virus has been detected. The error message includes the name of the virus, the sender of the e-mail, the date sent and the name of the infected file or the name of the compressed archive file and the infected portion of this archive.
An example of a virus message:

```
mGuard detected a virus. The mail could not be delivered.
found Virus Email-Worm.Win32.NetSky.q /[From
sick@example.com][Date Fri, 13 Aug 2004 11:33:53++0200]/
about_you.zip/document.txt.exe
[000012a7.00000077.00000000]
Message Details:
From: sick@example.com
Subject: Private document
Date: Fri, 13 Aug 2004 11:33:53 +0200
```

Exceeded maximum filesize
The maximum filesize set for this protocol was exceeded.
To transfer the file anyway, you can deactivate the virus filter either for the corresponding server for the course of the download or globally. Alternatively, you can set the “Action for ...exceeding the maximum message size” parameter to “Let the message/data pass unscanned” for the respective protocol.

⌦In either case, the transferred file will not be scanned for viruses.

Temporary Virus Scanner Failure
A temporary error occurred while trying to scan a file. It is possible that the problem will be cleared if you repeat the transfer again at a later time or if you update the virus signature file.
Possible causes:

- The scan-engine cannot process the file.
- The Innominate mGuard does not have enough memory available to decompress the file.
- Internal error in the scan-engine.

Exceptional Virus Scanner Failure
A problem has occurred in the communication with the scan-engine. For more details, please see the anti-virus log.
Possible causes:

- The information entered for the update server is faulty and the signature update has failed (see the “Basic Settings >Update” menu).
- Invalid virus filter license.
- Damaged or faulty update of the virus signature file.

Update running
There is currently no anti-virus database installed, and the download of the current database has been started. You can follow the progress of the download in the Diagnosis->Event Logs->AntiVirus Update menu.

DHCP Server/Relay

Messages from services defined under “Network > DHCP”.

Anti-Virus Update

The update log contains notifications regarding the start and progress of the update process for the virus signature files.

SNMP/LLDP

Messages from services defined under “Management > SNMP”.

IPsec VPN

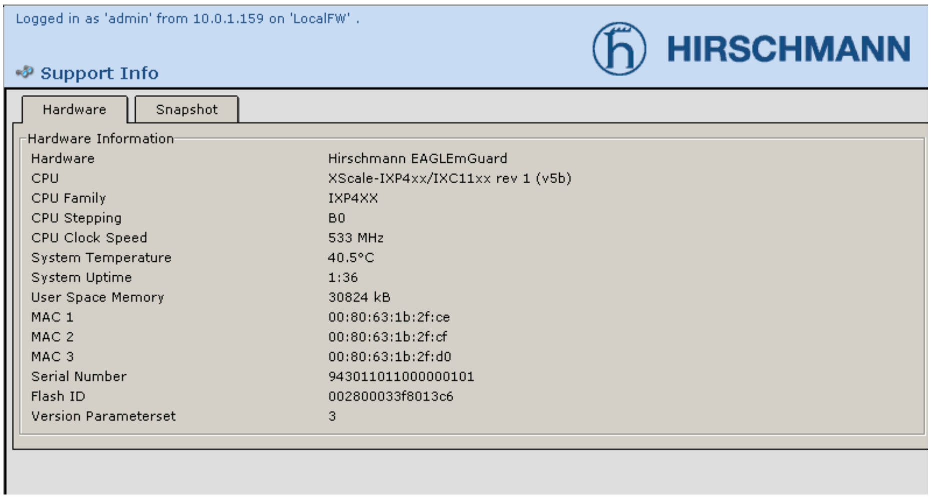
Lists all VPN events.

The format corresponds to the standard Linux format.

It offers special evaluation programs that present information from the logged data in a more readable format.

6.8.3 Diagnosis → Support Info

Hardware



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

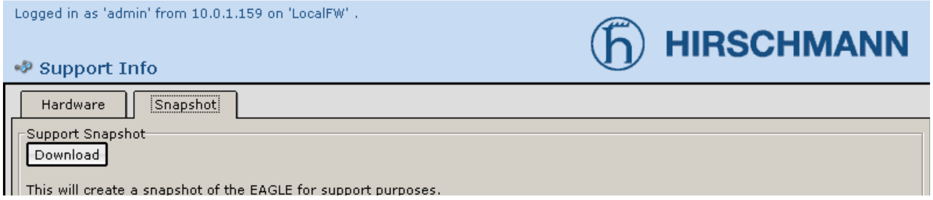
Support Info

Hardware Information

Hardware	Hirschmann EAGLEmGuard
CPU	XScale-IXP4xx/IXC11xx rev 1 (v5b)
CPU Family	IXP4XX
CPU Stepping	B0
CPU Clock Speed	533 MHz
System Temperature	40.5°C
System Uptime	1:36
User Space Memory	30824 kB
MAC 1	00:80:63:1b:2f:ce
MAC 2	00:80:63:1b:2f:cf
MAC 3	00:80:63:1b:2f:d0
Serial Number	943011011000000101
Flash ID	002800033f8013c6
Version Parameterset	3

This page lists the hardware properties of the mGuard.

Snapshot



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Support Info

Support Snapshot

Download

This will create a snapshot of the EAGLE for support purposes.

This function is intended to provide the support with the necessary diagnostic information.

This function prepares a compressed file (in tar format) containing all of the current configuration settings and log entries, which could be relevant to the diagnosis of errors. (This file does not contain any private information such as the private machine certificate or the passwords.)

To take a snapshot, proceed as follows:

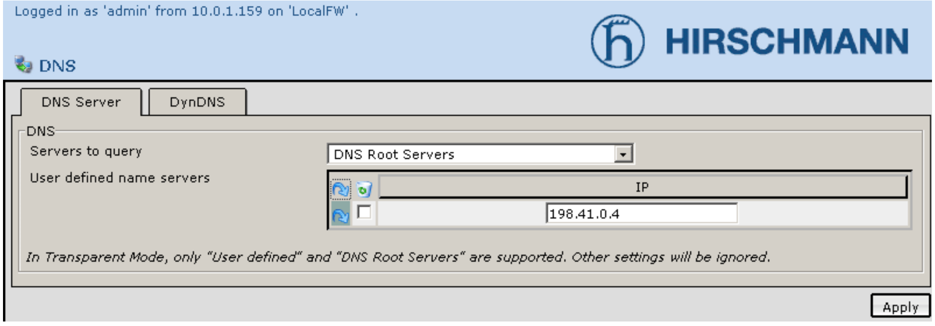
1. Click on **Download**.
2. Save the file under the name *snapshot.tar.gz*

Please make the file available to the support, if requested.

6.9 Extended

6.9.1 Extended → DNS

DNS Server



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

DNS

Servers to query: DNS Root Servers

User defined name servers

IP
198.41.0.4

In Transparent Mode, only "User defined" and "DNS Root Servers" are supported. Other settings will be ignored.

When the mGuard has to initiate a connection on its own to a remote system (e.g. a VPN gateway or a NTP server) and it is defined in form of a host name (i.e. in the form of www.example.com) then the mGuard has to query a domain name server (DNS) for the IP address belonging to the host name.

If the mGuard is not in stealth mode locally connected clients can be configured to use the mGuard itself as a DNS server. See "IP configuration on Windows clients" on page 133.

DNS

Servers to query

Possible settings:

- DNS Root Servers
- Provider defined (i.e. via PPPoE or DHCP)
- User defined (servers listed below)

DNS Root Servers:

Queries will be sent to the DNS Root server in Internet found at the IP address which is stored in the mGuard. These addresses rarely change.

Provider defined (e.g. via PPPoE or DHCP)

With this setting, the device will use the Domain Name Server of the Internet Service Provider, which is used to access the Internet. Only select this setting if the mGuard is operated in *PPPoE* or *PPTP* mode or in *Router* mode with DHCP.

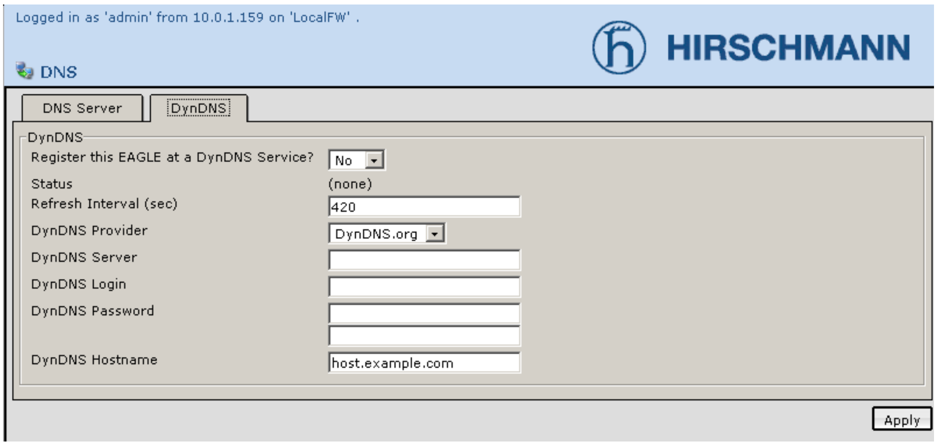
User defined (servers listed below)

If this setting is selected, the mGuard will connect to the Domain Name Servers shown in the list of *User defined name servers*.

User defined name servers

You can record the IP addresses of domain name servers in this list. If one of these should be used by the mGuard, select the option **User defined (servers listed below)** under *Servers to query*.

DynDNS



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

DynDNS

Register this EAGLE at a DynDNS Service?	No
Status	(none)
Refresh Interval (sec)	420
DynDNS Provider	DynDNS.org
DynDNS Server	
DynDNS Login	
DynDNS Password	
DynDNS Hostname	host.example.com

DynDNS

If a VPN connection is to be setup, at least the IP address of one of the partners must be known so that the other can setup a connection to it. This condition is not satisfied, if both sites/stations are assigned their IP addresses dynamically by their respective Internet Service Providers. In this case, a DynDNS-Service such as DynDNS.org or DNS4BIZ.com can be of assistance. The currently valid IP address of a site/station is registered under a fixed name at a DynDNS service.

If you have registered with one of the DynDNS services supported by mGuard, you can enter the corresponding information in this screen.

Register this mGuard at a DynDNS Service? Yes / No

Select **Yes**, if you have registered with a DynDNS provider and the mGuard should utilize this service. In this case, the mGuard will report its current IP address – the one assigned for its own Internet access by its Internet Service Provider – to the DynDNS Service.

Refresh Interval (sec)

Standard: 420 (seconds)

Whenever the IP address of its own Internet access is changed, the mGuard will inform the DynDNS Service of its new IP address. For additional reliability, the device will also report its IP address at the interval set here.

This setting is ignored for some DynDNS providers like DynDNS.org where too many updates will cause the account to be closed.

DynDNS Provider

The providers in the list support the same protocol as the mGuard.

Select the name of the provider with which you are registered, e.g. DynDNS.org.

DynDNS Server

The name of the server of the DynDNS provider selected above, e.g.: dyndns.org.

DynDNS Login, DynDNS Password

Enter the user name and password that you have been assigned by the DynDNS provider here.

DynDNS Hostname

The name selected at the DynDNS Service for this mGuard - if you use a DynDNS Service and have entered the corresponding data above.

6.9.2 Extended → DHCP

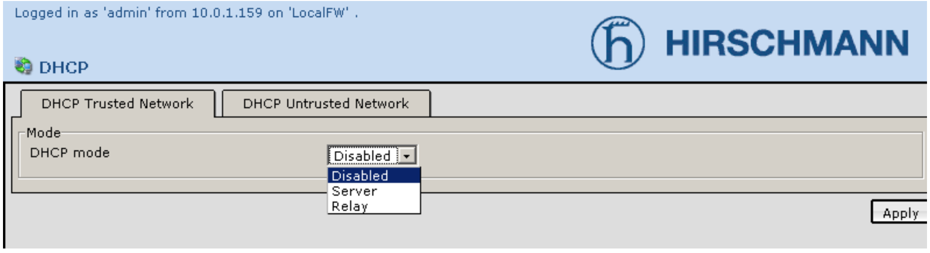
The Dynamic Host Configuration Protocol (DHCP) automatically assigns appropriate network parameters (like IP address or subnet mask) to the clients connected to the mGuard. Under DHCP Intern you can configure the settings for the internal interface (trusted port) and under DHCP Extern the settings for the external interface (untrusted port).

⌧The DHCP server/relay is also operational in Transparent mode.

⌧IP configuration on Windows clients

To do so, if you are using Windows XP, click on **Start, Control Panel**, **Network Connections**: Right click on the icon of the LAN adapter and then click on **Properties** in the pop-up menu. In the Internet Protocol Properties dialog on the General tab, select **Internet Protocol (TCP/IP)** under "This connection uses the following items" and then click on the **Properties** button. In the *Internet Protocol Properties (TCP/IP)* dialog, make the appropriate entries or settings.

Trusted/Untrusted DHCP



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

Mode

DHCP mode

Server

The mGuard will work as an independent DHCP server.

Relay

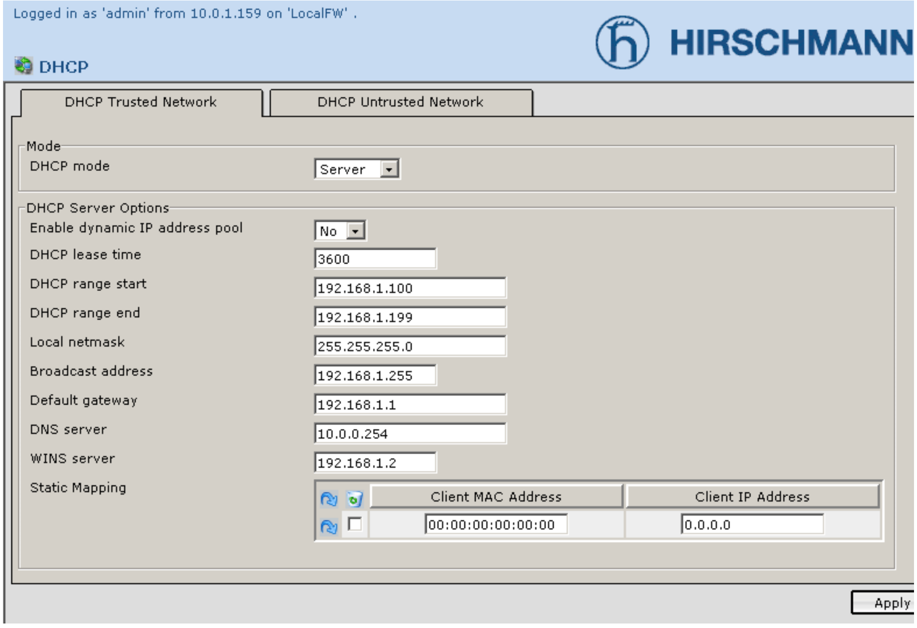
The mGuard will forward DHCP requests to other DHCP servers on its external interface (WAN).

Disabled

The mGuard will not answer DHCP requests.

⌧The DHCP server/relay is also operational in Transparent mode.

DHCP mode Server



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

DHCP

Mode

DHCP mode: Server

DHCP Server Options

Enable dynamic IP address pool: No

DHCP lease time: 3600

DHCP range start: 192.168.1.100

DHCP range end: 192.168.1.199

Local netmask: 255.255.255.0

Broadcast address: 192.168.1.255

Default gateway: 192.168.1.1

DNS server: 10.0.0.254

WINS server: 192.168.1.2

Static Mapping

Client MAC Address	Client IP Address
00:00:00:00:00:00	0.0.0.0

When the DHCP mode is set to Server the following options are available:

DHCP Server Options (Mode = Server)

Enable dynamic IP address pool

Select **Yes**, if you wish to use the dynamic IP address pool defined by **DHCP range start** and **DHCP range end**.

Select **No**, if you wish to use IP addresses statically assigned by the means of the MAC address (see below).

DHCP lease time

Time in seconds, for which the network configuration assigned to the client is valid. Briefly before expiration of this time the client should renew its configuration. Otherwise it may be assigned to another computer.

With enabled dynamic IP address pool:

When the DHCP server and the dynamic IP address pool has been activated, you can enter the network parameters that should be used by the client(s):

DHCP range start: **DHCP range end:**	The start and end of the address range from which the mGuard's DHCP server should assign IP addresses to its locally connected clients.
Local Netmask:	The factory setting is: 255.255.255.0
Broadcast IP:	The clients broadcast IP.
Default gateway:	This field is used to define which IP address should be used by the client(s) as the standard gateway. Usually this is the internal IP address of the mGuard.

DNS server: This field is used to define the Domain Name Service (DNS) server which the clients can access to find out the IP address that is associated with a specific domain name. If you would like to use the DNS service of the mGuard, use the internal address of the mGuard for this field

WINS-server: This field is used to define the Windows Internet Naming Service (WINS) server.

Static mapping

You can find out the MAC address of your client by using the following commands:

Windows 95/98/ME: Click on the **Start** button, and then click on **Run**. Type **winipcfg** in the Open box, and then click on **OK**. The MAC address will be shown as “Adapter Address”

NT/2000/XP: Select the **Start** button on the Task Bar. Select **Run**. Type **cmd.exe**. When the DOS command prompt window opens, type **ipconfig /all** The MAC address will be shown as “Physical Address”.

Linux: Start **/sbin/ifconfig** or **ip link show** in a shell.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 44.

You must enter the following data when assigning IP and MAC addresses:

Client MAC address

The MAC address of the client. Please enter without spaces or hyphens.

Client IP address

The IP address you wish to assign to the MAC address.

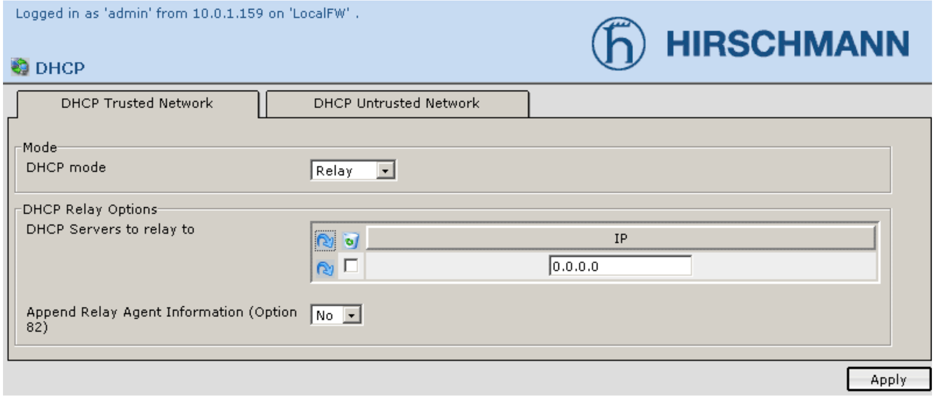
☞ The statically assigned IP addresses take priority over the dynamic IP address pool

☞ Static IP addresses and pool addresses must not overlap

☞ Do not assign one IP address to several MAC addresses, otherwise several clients will be assigned the same IP address

☞ You should only use one DHCP server per subnetwork.

DHCP mode Relay



Logged in as 'admin' from 10.0.1.159 on 'LocalFW' .

DHCP

DHCP Trusted Network | DHCP Untrusted Network

Mode

DHCP mode: Relay

DHCP Relay Options

DHCP Servers to relay to

IP
0.0.0.0

Append Relay Agent Information (Option 82): No

When the DHCP mode is set to Relay the following options are available:

DHCP Relay Options (Mode = Relay)

DHCP servers to relay to
A list of DHCP servers, to which DHCP requests are to be passed on.

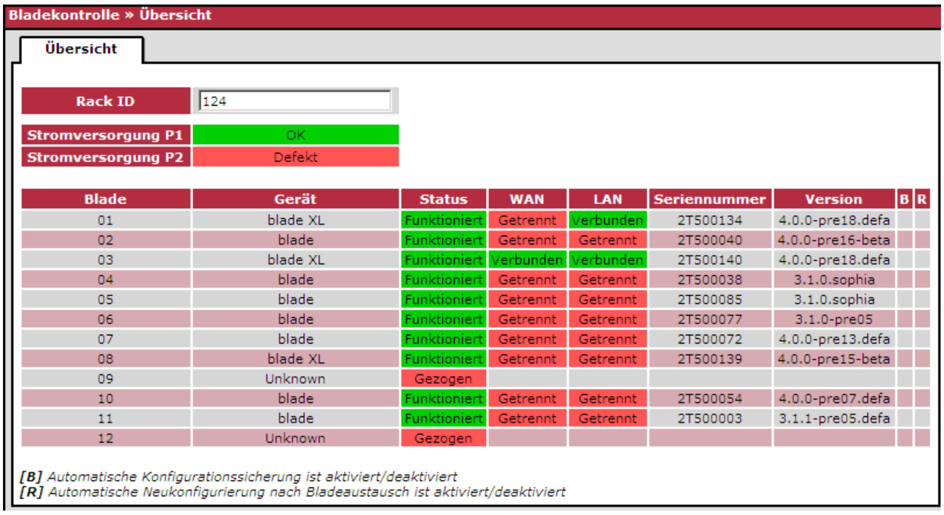
Append Relay Agent Information
When this option is set to **Yes**, additional information according to RFC 3046 will be added.

⌦IP configuration on Windows clients
To do so, if you are using Windows XP, click on **Start, Control Panel, Network Connections**: Right click on the icon of the LAN adapter and then click on **Properties** in the pop-up menu. In the *Internet Protocol Properties* dialog on the *General* tab, select **Internet Protocol (TCP/IP)** under "This connection uses the following items" and then click on the **Properties** button. In the *Internet Protocol Properties (TCP/IP)* dialog, make the appropriate entries or settings.

6.10 Menu Entry Blade Control (control unit only)

This menu is only available on the control unit.

6.10.1 *Blade control → Overview*



Rack ID	124
Stromversorgung P1	OK
Stromversorgung P2	Defekt

Blade	Gerät	Status	WAN	LAN	Seriennummer	Version	B	R
01	blade XL	Funktioniert	Getrennt	Verbunden	2T500134	4.0.0-pre18.defa		
02	blade	Funktioniert	Getrennt	Getrennt	2T500040	4.0.0-pre16-beta		
03	blade XL	Funktioniert	Verbunden	Verbunden	2T500140	4.0.0-pre18.defa		
04	blade	Funktioniert	Getrennt	Getrennt	2T500038	3.1.0.sophia		
05	blade	Funktioniert	Getrennt	Getrennt	2T500085	3.1.0.sophia		
06	blade	Funktioniert	Getrennt	Getrennt	2T500077	3.1.0-pre05		
07	blade	Funktioniert	Getrennt	Getrennt	2T500072	4.0.0-pre13.defa		
08	blade XL	Funktioniert	Getrennt	Getrennt	2T500139	4.0.0-pre15-beta		
09	Unknown	Gezogen						
10	blade	Funktioniert	Getrennt	Getrennt	2T500054	4.0.0-pre07.defa		
11	blade	Funktioniert	Getrennt	Getrennt	2T500003	3.1.1-pre05.defa		
12	Unknown	Gezogen						

[B] Automatische Konfigurationssicherung ist aktiviert/deaktiviert
[R] Automatische Neukonfigurierung nach Bladeaustausch ist aktiviert/deaktiviert

Rack ID

The ID of the rack into which the mGuard is mounted. This values can be set on the control unit for all blades inside the rack.

Power Supply P1/P2

State of the power supplies P1 and P2.

- OK
- Absent
- Defect
- Fatal Error

Blade

Number of the slot in which the mGuard is installed.

Device

Device type, e.g. “blade2 or “blade XL”.

State

Online The device in the slot is ready.

Present The device is present but not ready yet, e.g. it is still booting.

Absent No device was found in the slot.

WAN

Status of the Ethernet WAN port.

LAN

Status of the Ethernet LAN port.

Serial

The mGuard’s serial number.

Version

Software version of the mGuard.

B

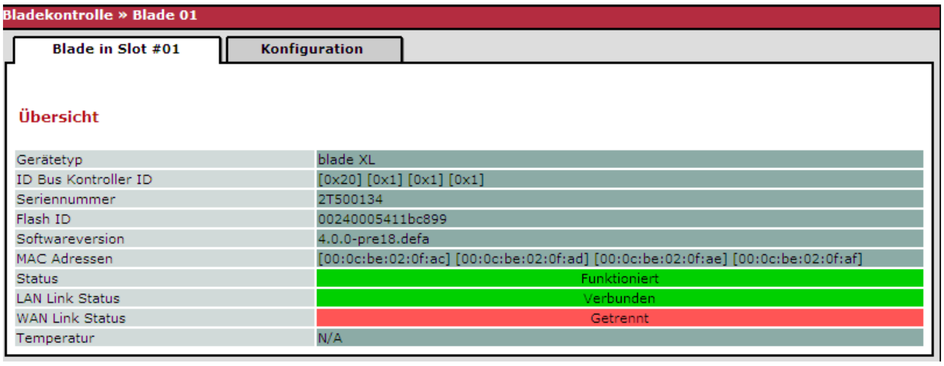
Automatic configuration **backup** on the controller is activated/deactivated for this slot.

R

Automatic configuration **restore** from the controller is activated/deactivated for this slot.

6.10.2 Blade control → Blade 01 to 12

Blade in slot #__



Bladekontrolle » Blade 01

Übersicht

Gerätetyp	blade XL
ID Bus Kontroller ID	[0x20] [0x1] [0x1] [0x1]
Seriennummer	2T500134
Flash ID	00240005411bc899
Softwareversion	4.0.0-pre18.defa
MAC Adressen	[00:0c:be:02:0f:ac] [00:0c:be:02:0f:ad] [00:0c:be:02:0f:ae] [00:0c:be:02:0f:af]
Status	Funktioniert
LAN Link Status	Verbunden
WAN Link Status	Getrennt
Temperatur	N/A

Overview

Device type

Device type, e.g. “blade” or “blade XL”.

ID bus Controller ID

ID of this slot on the bladeBases control bus.

Serial

The mGuard’s serial number.

Flash ID

Serial number of the mGuard’s flash chip.

Software version

Software version of the mGuard.

MAC addresses

All MAC addresses used by the mGuard.

Status

Status of the mGuard

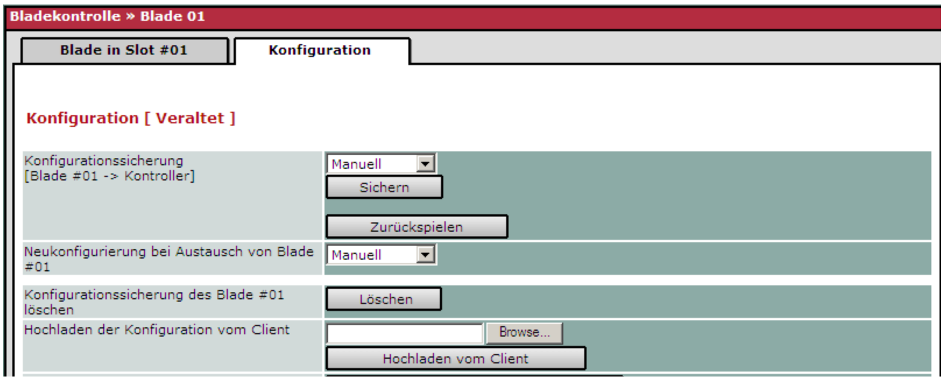
WAN link status

Status of the Ethernet WAN port.

LAN link status

Status of the Ethernet LAN port.

Configuration



Bladekontrolle » Blade 01

Konfiguration [Veraltet]

Konfigurationssicherung [Blade #01 -> Kontroller]	Manuell Sichern Zurückspielen
Neukonfigurierung bei Austausch von Blade #01	Manuell
Konfigurationssicherung des Blade #01 löschen	Löschen
Hochladen der Konfiguration vom Client	Browse... Hochladen vom Client

Configuration

Configuration backup [Blade #__ -> Controller]

Automatic Shortly after a configuration change on the mGuard, the new configuration will be stored automatically on the controller.

Manual With the **Backup** button the configuration can be stored on the controller and with the **Restore** button it can be restored from the controller onto the mGuard.

Reconfiguration, if Blade #__ is replaced

After replacing a mGuard in this slot, the configuration stored on the controller will be automatically applied to the new mGuard.

Delete configuration backup of Blade #__

Deletes the configuration stored on the controller for this slot.

Upload configuration from client

Upload a configuration profile for this slot to the controller.

Download configuration to client

Download the configuration profile stored on the controller for this slot.

6.11 CIDR (Classless InterDomain Routing)

IP netmasks and CIDR are notations, which define an address space containing multiple IP addresses. In this case, an address space in which the addresses follow one another sequentially is treated as a network.

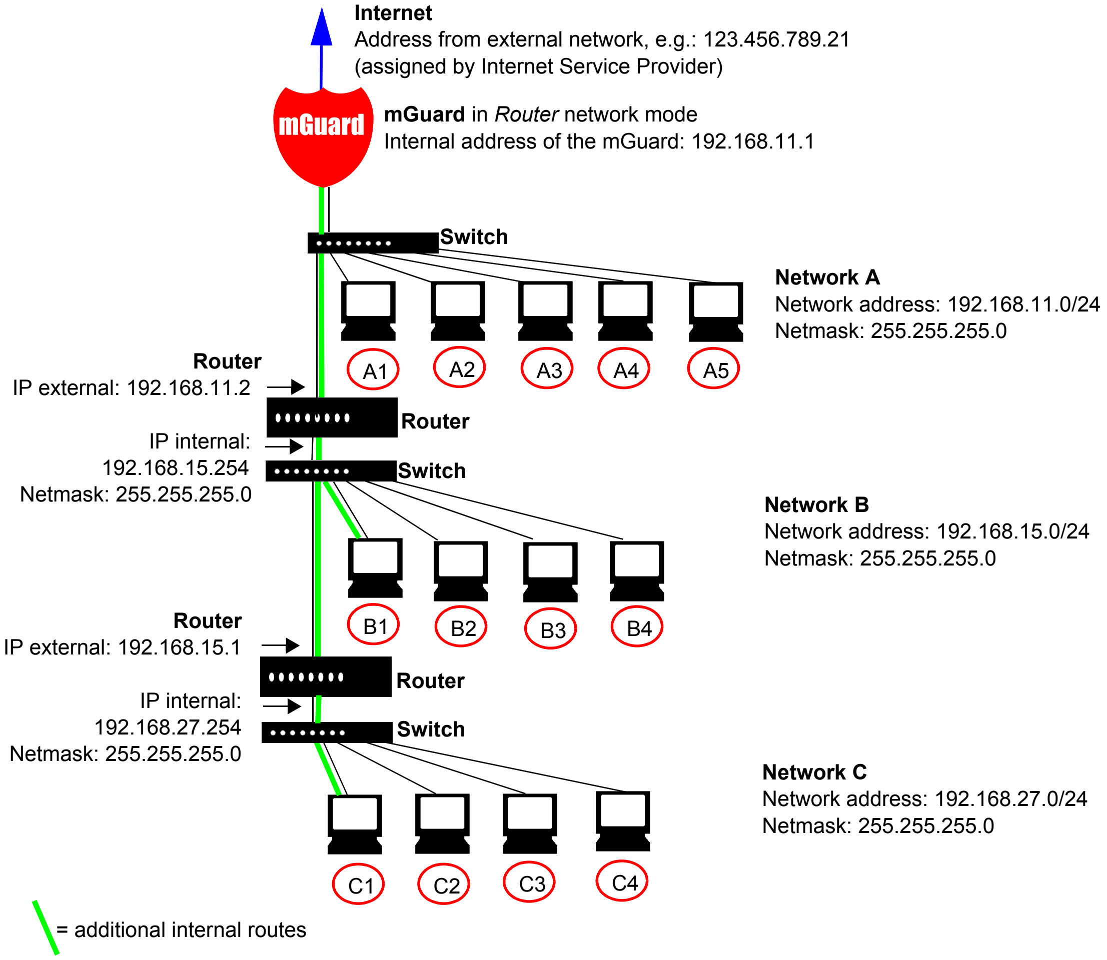
To define a range of IP addresses for the mGuard e.g. when configuring the firewall, it may be necessary to use the CIDR notation to specify the address space. The following table presents the IP netmask on the left and the corresponding CIDR notation on the right.

IP-Netmask	binary	CIDR
255.255.255.255	11111111 11111111 11111111 11111111	32
255.255.255.254	11111111 11111111 11111111 11111110	31
255.255.255.252	11111111 11111111 11111111 11111100	30
255.255.255.248	11111111 11111111 11111111 11111000	29
255.255.255.240	11111111 11111111 11111111 11110000	28
255.255.255.224	11111111 11111111 11111111 11100000	27
255.255.255.192	11111111 11111111 11111111 11000000	26
255.255.255.128	11111111 11111111 11111111 10000000	25
255.255.255.0	11111111 11111111 11111111 00000000	24
255.255.254.0	11111111 11111111 11111110 00000000	23
255.255.252.0	11111111 11111111 11111100 00000000	22
255.255.248.0	11111111 11111111 11111000 00000000	21
255.255.240.0	11111111 11111111 11110000 00000000	20
255.255.224.0	11111111 11111111 11100000 00000000	19
255.255.192.0	11111111 11111111 11000000 00000000	18
255.255.128.0	11111111 11111111 10000000 00000000	17
255.255.0.0	11111111 11111111 00000000 00000000	16
255.254.0.0	11111111 11111110 00000000 00000000	15
255.252.0.0	11111111 11111100 00000000 00000000	14
255.248.0.0	11111111 11111000 00000000 00000000	13
255.240.0.0	11111111 11110000 00000000 00000000	12
255.224.0.0	11111111 11100000 00000000 00000000	11
255.192.0.0	11111111 11000000 00000000 00000000	10
255.128.0.0	11111111 10000000 00000000 00000000	9
255.0.0.0	11111111 00000000 00000000 00000000	8
254.0.0.0	11111110 00000000 00000000 00000000	7
252.0.0.0	11111100 00000000 00000000 00000000	6
248.0.0.0	11111000 00000000 00000000 00000000	5
240.0.0.0	11110000 00000000 00000000 00000000	4
224.0.0.0	11100000 00000000 00000000 00000000	3
192.0.0.0	11000000 00000000 00000000 00000000	2
128.0.0.0	10000000 00000000 00000000 00000000	1
0.0.0.0	00000000 00000000 00000000 00000000	0

Example: 192.168.1.0 / 255.255.255.0 corresponds to 192.168.1.0/24 in CIDR notation

6.12 Network Sketch

The following sketch illustrates, how the IP addresses can be distributed in a local network with subnets, which network addresses result and how the details regarding additional internal routes might look.


Internet
Address from external network, e.g.: 123.456.789.21
(assigned by Internet Service Provider)
mGuard
mGuard in *Router* network mode
Internal address of the mGuard: 192.168.11.1
Switch
Network A
Network address: 192.168.11.0/24
Netmask: 255.255.255.0
A1
A2
A3
A4
A5
Router
IP external: 192.168.11.2
Router
IP internal:
192.168.15.254
Netmask: 255.255.255.0
Switch
Network B
Network address: 192.168.15.0/24
Netmask: 255.255.255.0
B1
B2
B3
B4
Router
IP external: 192.168.15.1
Router
IP internal:
192.168.27.254
Netmask: 255.255.255.0
Switch
Network C
Network address: 192.168.27.0/24
Netmask: 255.255.255.0
C1
C2
C3
C4
= additional internal routes

Network A

System	A1	A2	A3	A4	A5
IP address	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Network B

System	B1	B2	B3	B4
IP address	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Network C

System	C1	C2	C3	C4
IP address	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Additional internal routes

Network:
192.168.15.0/24
Gateway
192.168.11.2

Network:
192.168.27.0/24
Gateway
192.168.11.2

7 The Rescue Button – restart, recovery procedure and to flash the firmware

The Rescue Button is used to set the device in one of the following states:

7.1 Performing a Restart

Objectives To restart the device using the configured settings.

Action: Press the **Rescue Button** for ca. 1.5 seconds, e.g. with a straightened paperclip:

- blade, PCI: until both red LEDs light
- delta: until the *Status* LED stops blinking
- EAGLE: until the *Status* LED and the *Link*-LEDs go off
- smart: until the middle LED lights up in red.

OR

Disconnect the power briefly. Restart the computer containing the mGuard PCI card.

7.2 Performing a Recovery

Objectives This is used to reset the mGuard to the **Transparent** network mode (mode of operation) so that it can again be accessed (for the purpose of configuring it) at the following address: **https://1.1.1.1/**
The mGuard delta and the mGuard blade Control Unit will be reset to Router-Mode and will be accessible at the internal interface at 192.168.1.1

⌧ The passwords and the settings configured for VPN connections and the firewall are retained.

Possible reasons for starting the Recovery procedure:
The mGuard is in Router or PPPoE mode and
– the mGuard’s IP address has been changed from the default setting and
– you don’t know the device’s current IP address.

Action:

1. Press the **Rescue Button** slowly 6 times (once per second).
2. 2. After about two seconds, the mGuard will respond:

- blade, PCI
  - On success the LAN LED lights green
  - On failure the WAN LED lights red
- delta
  - On success the Status LED lights green
  - On failure the Status LED stays dark
- EAGLE
  - On success the STATUS LED lights yellow
  - On failure the FAULT LED lights red
- smart
  - On success the middle LED lights green
  - On failure the middle LED lights red

3. Press the **Rescue Button** slowly 6 times again.
4. On success the device will perform a restart and switch to *Transparent* mode. It can then once again be accessed at the following address: **https://1.1.1.1/**
   The mGuard delta and the mGuard blade Control Unit will be switched to Router-Mode and will be accessible at 192.168.1.1 at the internal interface

7.3 Flashing the firmware

Objectives To reload the mGuard’s complete firmware.

⌦**All of the configured settings will be deleted.** The mGuard will be restored to the factory (default) settings.

Possible reasons for flashing the firmware:

- The Administrator and Root password have been lost.

Action: Proceed as follows:

⌦**Do not interrupt the power supply during the flashing procedure. Otherwise the device could be damaged and may be left inoperable, and will require your device to be send to the manufacturer.**

Prerequisites:

- First copy the mGuard software from the mGuard CD-ROM or retrieve it from Innominate Support and save it on the configuration system.
- A DHCP and a TFTP server, both installed on a single system, which provide the mGuard image files – see “Required before the firmware can be flashed: DHCP and TFTP servers” on page 145.
- mGuard PCI: When the mGuard is in Power-over-PCI mode the DHCP/TFTP server must be connected to the mGuards LAN jack. When the mGuard is in PCI mode the DHCP/TFTP server must listen on the mGuards network interface.

1. Hold the Rescue Button pressed until the recovery status is entered as follows:

The mGuard will be restarted (after approx. 1.5 seconds) and after another approx. 1.5 seconds the mGuard will enter the recovery mode:

- blade, PCI: the green and the red LAN will light
- delta: the Status LED will slowly fade darker
- EAGLE: the LEDs 1, 2 and V.24 will light
- smart: all LEDs will light green

2. No more than 1 second after the recovery mode was entered release the **Resuce Button**. (If you do not release the **Rescue Button** quickly enough, the mGuard will restart again.)

   The mGuard will now start the recovery system: He tries to receive an IP address from an DHCP server over the LAN port.

- Status display:
  - blade, PCI: the red LAN LED flashes
  - delta: the Status LED flashes
  - EAGLE: the LEDs 1, 2 and V.24 light orange
  - smart: the middle LED (heartbeat) flashes.

  The file install.p7s will be loaded from the TFTP server, which contains the installation procedure for the flashing. (Only files digitally signed by Innominate will be accepted.)

  Afterwards the flash memory will the be erased.
- Status display:
  - blade, PCI: the two green and the red LAN LED form a bouncing ball display in which the light shifts from one LED to the next.
  - delta: the Status LED will flash fast.
  - EAGLE: the LEDs 1, 2 and V.24 form a bouncing ball display in which the light shifts from one LED to the next.
  - smart: the 3 green LEDs form a bouncing ball display in which the light shifts from one LED to the next

  The file jffs2.img.p7s which contains the mGuard software will be loaded from the TFTP server and written onto the flash. (Only files digitally signed by Innominate will be accepted.)

  This process will take about 3 to 5 minutes.

  - Status display:
  - blade, PCI: the green and the red LEDs will flash continuously
  - delta: the Status LED will light continuously
  - EAGLE: the LEDs 1, 2 and V.24 are off, the LEDs P1, P2 and Status will light continuously
  - smart: the middle LED (heartbeat) will light continuously

  The new software will be unpacked and configured. This process will take about 5 minutes.

  As soon as the procedure has been completed

  - blade, PCI: the mGuard restarts itself
  - delta: the Status LED will flash once per second continuously
  - EAGLE: the LEDs 1, 2 and V.24 will flash green continuously
  - smart: all 3 LEDs will flash green continuously

3. Restart the mGuard (not required on blade and PCI)

   To do so, press the **Rescue Button** briefly.

   OR

   Disconnect the power supply (smart: by disconnecting the USB cable which is only used to supply power) or in case of the mGuard PCI: restart the computer.

The mGuard will be now restored to its factory settings. Configure it once again – see “Local Configuration: At startup” on page 34.

Required before the firmware can be flashed: DHCP and TFTP servers

Before the firmware can be “flashed” DHCP and TFTP servers must be installed on the locally connected system or a network system.
(DHCP = **D**ynamic **H**ost **C**onfiguration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Install the DHCP and TFTP server, if necessary (see below).
⌦ If you install a second DHCP server in a network, this can affect the configuration of the entire network!

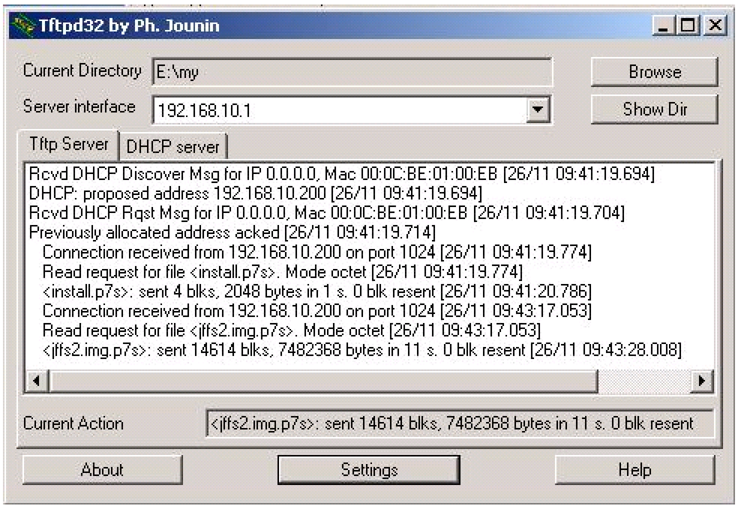
7.3.1 Installing DHCP and TFTP servers under Windows or Linux

Under Windows: Install the program found on the CD-ROM. To accomplish this, proceed as follows:

1. If the Windows system is connected to a network, disconnect it.
2. Copy the software into any empty folder on the Windows system. Start the program TFTPD32.EXE
3. The system’s IP must be set to: **192.168.10.1.** This must also be the address of the network adapter.

   Click on the **Browse** button to switch to the folder in which the mGuard image files have been saved: *install.p7s, jffs2.img.p7s*

The image files are also found on the CD-ROM, which was included in the package.



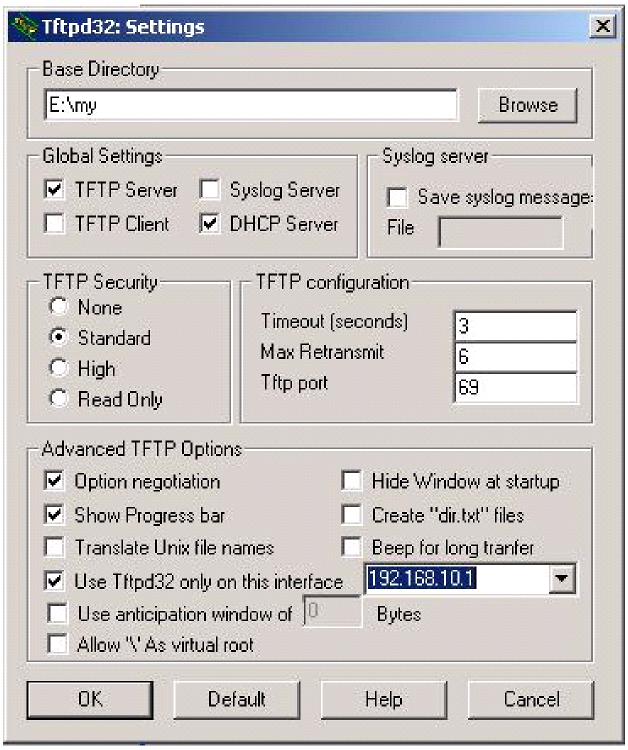
Current Directory: E:\my

Server interface: 192.168.10.1

```
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.694]
DHCP: proposed address 192.168.10.200 [26/11 09:41:19.694]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.704]
Previously allocated address acked [26/11 09:41:19.714]
  Connection received from 192.168.10.200 on port 1024 [26/11 09:41:19.774]
  Read request for file <install.p7s>. Mode octet [26/11 09:41:19.774]
  <install.p7s>: sent 4 blks, 2048 bytes in 1 s. 0 blk resent [26/11 09:41:20.786]
  Connection received from 192.168.10.200 on port 1024 [26/11 09:43:17.053]
  Read request for file <jffs2.img.p7s>. Mode octet [26/11 09:43:17.053]
  <jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent [26/11 09:43:28.008]
```

Current Action: <jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent

4. Click on the TFTP Server or DHCP Server tab and then click on the Settings button to open the dialog shown below. Then set the parameters as shown:



Base Directory: E:\my

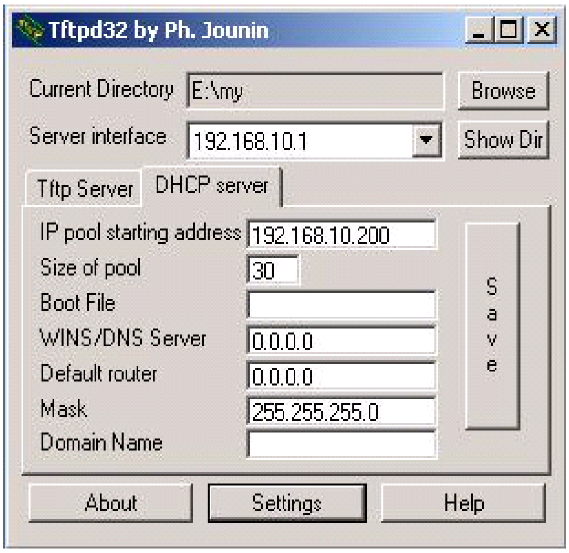
Global Settings:
☑ TFTP Server ☐ Syslog Server
☐ TFTP Client ☑ DHCP Server

Syslog server: ☐ Save syslog message; File:

TFTP Security: ○ None ● Standard ○ High ○ Read Only

TFTP configuration: Timeout (seconds) 3; Max Retransmit 6; Tftp port 69

Advanced TFTP Options:
☑ Option negotiation ☐ Hide Window at startup
☑ Show Progress bar ☐ Create "dir.txt" files
☐ Translate Unix file names ☐ Beep for long tranfer
☑ Use Tftpd32 only on this interface 192.168.10.1
☐ Use anticipation window of 0 Bytes
☐ Allow '\' As virtual root



Current Directory: E:\my

Server interface: 192.168.10.1

IP pool starting address: 192.168.10.200

Size of pool: 30

Boot File:

WINS/DNS Server: 0.0.0.0

Default router: 0.0.0.0

Mask: 255.255.255.0

Domain Name:

Under Linux

All current Linux distributions include DHCP and TFTP servers. Install the corresponding packages as described in the instructions for the respective distribution.
Configure the DHCP server by making the following settings in the **/etc/dhcp file**:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.134.255;}
```

This sample configuration makes 20 IP addresses (.100 to .119) available. It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file:

/etc/inetd.conf

In this file, insert the appropriate lines or set the necessary parameter for the TFTP service. (The directory for the data is: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

Then restart the inetd process to activate the modified configuration.
If you use a different mechanism, e.g. xinetd, please read the corresponding documentation.

8 Glossary

Asymmetrical encryption

In the case of asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Either key may be used for encryption or decryption. One of the keys is kept secret by its owner (Private Key), the other is made available to the public (Public Key), i.e. possible communication partners.

A message encrypted with the public key can only be decrypted and read by the owner of the associated private key. A message encrypted with the private key can only be decrypted and read by a receiver who has the associated public key. The fact that the message was encrypted with the private key proves that the owner of the associated public key actually sent the message. Therefore, the expression "digital signature" is also often used.

However, asymmetrical encryption techniques such as RSA are both slow and susceptible to certain types of attack and are therefore frequently combined with some form of symmetrical encryption (→ symmetrical encryption). On the other hand, there are concepts which avoid the additional work of administering symmetrical keys.

DES / 3DES

This symmetrical encryption algorithm was developed by IBM and checked by the NSA. DES (→ symmetrical encryption) was set in 1977 by the American National Bureau of Standards, which was the predecessor of the National Institute of Standards and Technology (NIST), as the standard for American governmental institutions. Since this was the very first standardized encryption algorithm, it quickly won acceptance by industry even outside of America.

DES uses a 56 bit long key, which is no longer considered secure as the processing power available has greatly increased since 1977.

3DES is a variant of DES. It uses keys that are three times as long, i.e. 168 bits long. 3DES is still considered to be secure and is also included in the IPsec standard.

AES

Advanced Encryption Standard. This encryption standard was developed by NIST (National Institute of Standards and Technology) in cooperation with the industry. This → symmetrical encryption standard was developed to replace the earlier DES standard. AES specifies three different key sizes (128, 192 and 256 bits).

In 1997, NIST started the AES initiative and announced its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination – the MARS, RC6, Rijndael, Serpent and Twofish algorithms. In October 2000, the Rijndael algorithm was adopted as the standard‘s encryption algorithm.

Client / Server

In a client-server environment, a server is a program or computer, which accepts and answers queries from client programs or computers.

In data communication, a computer which establishes a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

Datagram

In the IP protocol, data is sent in the form of data packets, which are known as IP datagrams. An IP datagram has the following structure:

IP Header	TCP, UDP, ESP etc. Header	Data (Payload)

The IP header contains:

– the IP address of the sender (source IP address)
– the IP address of the receiver (destination IP address)
– the protocol number of the protocol of the next higher protocol layer (in accord with OSI [seven layer] model)
– the IP header checksum used to check the integrity of the received header.
The TCP/UDP header contains the following information:
– the sender’s port (source port)
– the recipient’s port (destination port)
– a checksum covering the header and some information from the IP header (among others the source and destination IP addresses)

Default route

If a computer is connected to a network, the operating system creates a routing table internally. It lists the IP addresses that the operating system has identified based on the connected computers and the routes available at that moment. Thus the routing table contains the feasible routes (destinations) for sending IP packets. If IP packets are ready for sending, the computer’s operating system compares the IP addresses stated in the IP packets with the entries in the routing table to determine the right route.

If a router is connected to the computer, and if its internal IP address (i.e., the IP address of the router’s LAN port) has been relayed to the operating system as the standard gateway (in the network card’s TCP/IP configuration), this IP address will be used as the destination if all other IP addresses in the routing table don’t match. In this case the router’s IP address specifies the default route, because all IP packets (by default = the standard) whose IP address have no counterpart in the routing table, i.e., can't find a route, are directed to this gateway.

DynDNS provider

Also *Dynamic DNS provider*. Every computer, which is connected to the Internet, has an IP address (IP = Internet Protocol). An IP address consists of a maximum of 4 three-digit numbers, which are each separated by a dot. If the computer accesses its Internet Service Provider (ISP) via a modem on a phoneline, ISDN or ADSL, its ISP will assign it a dynamic IP address. In other words, it will be assigned a different address for every online session. If the computer is online 24 hours a day without interruption (e.g. in the case of a flat rate access), the IP address will even change during the session.
If a local computer should be accessible via the Internet, it must have an address that is known to the remote system. Unless this is true no connection can be established between the remote system and the local computer. If the local computer‘s address is constantly changing, no connection can be setup. Unless, of course, the operator of the local computer has an account with a Dynamic DNS provider (DNS = Domain Name Server).
In this case, the operator can set a host name with this provider under which the system should be reachable, e.g.: www.example.com. The Dynamic DNS provider also supplies a small program, which must be installed and run on this local computer. At each new Internet session, this tool will inform the Dynamic DNS provider which IP address the local computer has currently been assigned. This Domain Name Server will register the current assignment of Domain Name - IP Address and will also inform the other Domain Name Servers in the Internet.
Now, if a remote system wishes to establish a connection to a local system, which is registered with the DynamicDNS provider, the remote system can use the host name of the local system as its address. This will setup a connection to the responsible DNS (Domain Name Server) to lookup the IP address that is currently registered for this hostname. The corresponding IP address will be

sent back from the DNS to the remote system, which can then use this as the destination address. The remote system can now directly address the desired local computer.
In principle, all Internet addresses are based on this procedure: First, a connection will be established to a DNS to lookup the IP address assigned for the domain name. Once that has been accomplished, this “looked up” IP address will be used to setup a connection to the desired remote site, which could be any site in the Internet.

IP address

Every host or router in the Internet or an Intranet has a unambiguous IP address (IP = Internet Protocol). The IP address is 32 bits (= 4 bytes) long and is written as 4 three-digit numbers (each in the range from 0 to 255), which are separated by a dot.
An IP address consists of 2 parts: the network address and the host address.

Network Address	Host Address

Each host [or workstation] in a network has the same network address, but a different host address. Depending on the size of the respective network – networks are categorized as Class A, B or C networks, which are each different in size – the two parts of the address differ in length:

	1. Byte	2. Byte	3. Byte	4. Byte
Class A	Network Address	Host Address		
Class B	Network Address		Host Address	
Class C	Network Address			Host Address

Whether the IP address of device in a network is Class A, B or C can be seen in the first byte of the IP address. The following has be specified:

	Value of the 1st Byte	No. of bytes for the network address	No. of bytes for the host address
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

As you can see, there can be a worldwide total of 126 Class A networks and each of these networks can have a maximum of 256 x 256 x 256 hosts (3 bytes of address space). There can be 64 x 256 Class B networks and each of these networks can have up to 65,536 hosts (2 bytes address space: 256 x 256). There can be 32 x 256 x 256 Class C networks and each of these networks can have up to 256 hosts (1 bytes address space).

Subnet Mask

Normally, a company’s network - with access to the Internet - is only officially assigned a single IP address, e.g. 123.456.789.21. Based on the first byte of this sample address, one can see that this company network is a Class B network and therefore the last 2 bytes are free to be used for host addresses. With a Class B network, the company network has address space for up to 65,536 hosts (256 x 256).

Obviously, such huge network is not practical. At this point, one can see a need for subnetworks. The standard answers this need with the Subnet Mask. Like an IP address, this mask is 4 bytes long. The bytes, which represent the network address, are each assigned the value 255. The main purpose of the mask is to "borrow" a portion of the host address which can then be used to address the subnetworks. As an example, by using the subnet mask 255.255.255.0 in a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnet addressing. With this configuration, the company's network could support 256 subnetworks that each have 256 hosts.

IPsec

IP Security (IPsec) is a standard, which uses encryption to verify the authenticity of the sender and to ensure the confidentiality and integrity of the data in IP datagrams (→ Datagram). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA) and the Internet Key Exchange (IKE).

At the start of the session, systems which wish to communicate must determine which technique shall be used and the implications of this choice for the session e.g. *Transport Mode* or *Tunnel Mode*

In *Transport Mode*, an IPsec header will be inserted between the IP header and the TCP or UDP header respectively in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for a host- to-host connection.

In *Tunnel Mode*, an IPsec header and a new IP header will be added in front of the entire IP datagram. As a consequence, the original datagram will be encrypted in its entirety and sent as the payload of the new datagram.

The *Tunnel Mode* is used in VPN applications: The devices at the tunnel ends ensure that the datagrams are encrypted before they pass through the tunnel so the actual datagrams are completely protected while being transferred over the public network.

NAT (Network Address Translation)

Using Network Address Translation (NAT) – which is also often called *IP-Masquerading* – an entire network is "hidden" behind a single device, which is know as a NAT router. The internal computers in the local network with their IP addresses will remain hidden, if you communicate with the outside via a NAT router. The remote system will only see the NAT router with its own IP address.

If the internal computers are to directly communicate with external systems (in the Internet), the NAT router must modify the IP datagrams that are passed back-and-forth between the internal computers and the remote sites.

If an IP datagram is sent from the internal network to a remote site, the NAT router will modify the UDP and TCP headers respectively of the outgoing datagrams. It replaces the source IP address and port with its own IP address and - thus far unused - port. It maintains a table in which the original values are listed together with the corresponding new ones.

When a reply datagram is received, the NAT router will recognize that it is actually for an internal computer from the datagram's destination port. Using the table, the NAT router will replace the destination IP address and port and pass the datagram on via the internal network.

Port Number

The UDP and TCP protocols assign a port number to each peer participating in the connection. This way it becomes possible to handle more than one UDP or TCP connection between two peers at the same time.

Fixed port numbers are assigned for certain, frequently used application processes. These are called a “Assigned Numbers”. E.g. HTTP connections are usually established to TCP port 80 or POP3 connections to port 110.

PPPoE

The acronym for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. This protocol is based on the PPP and Ethernet standards. PPPoE defines how to connect users via Ethernet with the Internet via a jointly used broadband medium such as DSL, a Wireless LAN or a cable modem.

PPTP

The acronym for **P**oint-to-**P**oint **T**unneling **P**rotocol. This protocol was developed in a cooperation between Microsoft, U.S. Robotics and others to securely transfer data between VPN nodes (→ VPN) via a public network.

X.509 Certificate

A type of "Seal", which certifies the authenticity of a public key (→ asymmetrical encryption) and the associated data.

To enable the user of the public key, which will be used to encrypt the data, to be sure that the public key that he/she has received is really from its issuer and thus from the instance, which should later receive the data, it is possible to use certification. A *Certification Authority – CA* certifies the authenticity of the public key and the associated link between the identity of the issuer and his/her key. The certification authority will verify authenticity in accordance with its rules, which may, for example, require that the issuer of the public key appear before it in person. Once authenticity has be successfully certified, the certification authority will add its digital signature to the issuer’s public key. The result is a Certificate.

An X.509(v3) Certificate thus includes a public key, information about the key owner (given as it Distinguished Name (DN)), the authorized usage etc. and the signature of the certification authority.

The signature is created as follows: The certification authority creates an individual bit sequence, which is known as the HASH value, from the bit sequence of the public key, the information about its owner and other data. This sequence may be up to 160 bits long. The certification authority encrypts this with its own private key and then adds it to the certificate. The encryption with the certification authority's private key proves the authenticity of the certificate, i.e. the encrypted HASH string is the certification authority's digital signature. If the certificate's data is altered, this HASH value will no longer be correct with the consequence that the certificate will be worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the certification authority's private key, anyone who has the public key can decrypt the bit sequence and thus verify the authenticity of this fingerprint or signature.

The usage of a certification authority means it is not necessary for each owner of a key to know every other owner. It is enough for them to know the certification authority. The additional information about the key further simplifies the administration of the key.

X.509 certificates are used, e.g. for e-mail encryption, in S/MIME or IPsec.

Protocol, communication protocol

Devices, which communicate with each other, must follow the same rules. They must “speak the same language”. Such rules and standards are called protocols or communication protocols. Some of the more frequently used protocols include, for example, IP, TCP, PPP, HTTP and SMTP.

Proxy

A proxy (representative) is an intermediary service. A web proxy (e. g., Squid) is commonly placed upstream of a larger network. For example, if 100 employees accessed a certain website at the same time and did this via the web proxy, then the proxy would load the respective pages from the server only once and distribute them to the said employees. This reduces the outgoing traffic which, in turn, cuts down on costs.

Service Provider

Service providers are companies or institutions, which offer users access to the Internet or an online service.

Spoofing, Antispoofing

In Internet terminology, spoofing means supplying a false address. With the false Internet address, the user can create the illusion of being an authorized user.
Anti-Spoofing is term for mechanisms, which detect or prevent spoofing.

Symmetrical encryption

In the case of symmetrical encryption, the same key is used to encrypt and decrypt the data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but as the number of users increases the administration becomes rather involved.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

This is a family of network protocols. It is used to connect two computers in the Internet.
IP is the base protocol.
UDP is based on IP and sends individual packets. The packets may arrive at the recipient in an order different from that in which they were sent or they may even be lost.
TCP secures the connection and ensures, for example, that data packets are passed on the application in the right order.
UDP and TCP add the Port Numbers 1 to 65535 to the IP Addresses. The various services offered by the protocols may be distinguished by these Port Numbers.
A number of additional protocols are based on UDP and TCP, e.g. HTTP (HyperText Transfer Protocol), HTTPS (Secure HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3) and DNS (Domain Name Service).
ICMP is based on IP and adds control messages.
SMTP is an e-mail protocol that is based on TCP.
IKE is an IPsec protocol that is based on UDP.
ESP is an IPsec protocol that is based on IP.
On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) handles both protocols.
(➔ Datagram)

Trap

The SNMP protocol (Simple Network Management Protocol) is used in addition to the other protocols, especially in large networks. This UDP-based protocol is used for the central administration of network devices. For example, you can use the GET command to request a configuration or employ the SET command to change the configuration of a device, provided that the addressed network device is SNMP compliant. An SNMP-compliant device can also send SNMP messages independently, in case, for example, an extraordinary event should occur. Messages like this are called SNMP traps.

VLAN

A VLAN (Virtual Local Area Network) divides a physical network into several independent logical networks.
Devices within a VLAN can only access devices within their own VLAN. The membership to a LAN is defined by the physiacl network topology and the VLAN ID (1-4094).

All devices with the same VLAN ID belong to the same VLAN and can therefore communicate with each other.

For a VLAN (based on IEEE 802.1Q) the ethernet frame is extended by 4 bytes, with 12 bits containing the VLAN ID. The VLAN IDs “0” and “4095” are reserved and can’t be used for VLAN identification.

VPN (Virtual Private Network)

A **V**irtual **P**rivate **N**etwork (VPN) connects several separate private networks (subnets) together via a public network, e.g. the Internet, to form a single joint network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN thus offers an economical alternative to using dedicated lines to build a nationwide corporate network.